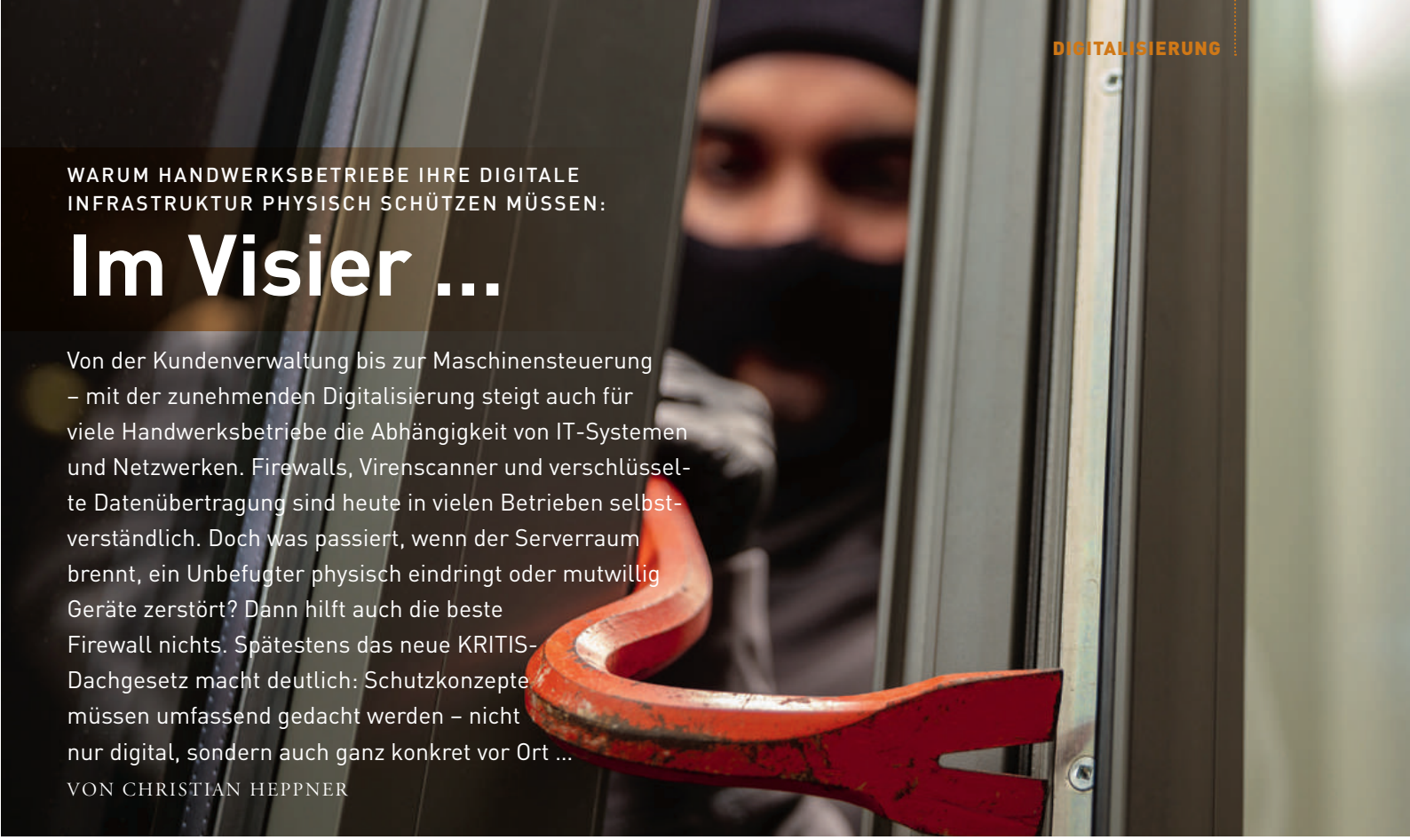

WARUM HANDWERKSBETRIEBE IHRE DIGITALE INFRASTRUKTUR PHYSISCH SCHÜTZEN MÜSSEN:

Im Visier ...

Von der Kundenverwaltung bis zur Maschinensteuerung – mit der zunehmenden Digitalisierung steigt auch für viele Handwerksbetriebe die Abhängigkeit von IT-Systemen und Netzwerken. Firewalls, Virenscanner und verschlüsselte Datenübertragung sind heute in vielen Betrieben selbstverständlich. Doch was passiert, wenn der Serverraum brennt, ein Unbefugter physisch eindringt oder mutwillig Geräte zerstört? Dann hilft auch die beste Firewall nichts. Spätestens das neue KRITIS-Dachgesetz macht deutlich: Schutzkonzepte müssen umfassend gedacht werden – nicht nur digital, sondern auch ganz konkret vor Ort ...

VON CHRISTIAN HEPPNER

Ob digitale Zeiterfassung, vernetzte Fertigungsmaschinen oder cloudbasierte Kundenakten: In modernen Handwerksbetrieben laufen viele Prozesse über Server oder Netzwerkspeicher, die zentral oder dezentral betrieben werden. Besonders kleinere Unternehmen setzen oft auf eine eigene IT-Infrastruktur – sei es im Keller, im Büro oder auf dem Firmengelände. Diese Technik ist nicht nur teuer, sondern in ihrer Funktion oft unternehmenskritisch. Denn häufig fehlt es an einem strukturierten physischen Sicherheitskonzept.

KRITIS-Dachgesetz: Relevanz auch unterhalb der Schwellenwerte

Um das Risiko des Ausfalls der eigenen Leistung durch Schäden zu minimieren, etabliert das KRITIS-Dachgesetz erstmals umfassende Vorgaben zur physischen Sicherheit und Resilienz kritischer Infrastrukturen in Deutschland, indem es eine EU-Richtlinie (EU 2022/2557, „CER-Richtlinie“) in nationales Recht umsetzt. Für betroffene Unternehmen, die mehr als 500.000 Menschen versorgen, bedeutet das, daß sie künftig nicht nur ihre IT-Systeme schützen, sondern auch Vorkehrungen gegen Stromausfälle, Sabotageakte oder andere nicht-digitale Gefahren treffen müssen. Erstmals wird eine ganzheitliche Sicherheitsbetrachtung verlangt, die alle Gefahrenarten – von Naturkatastrophen über technisches Versagen bis hin zu vorsätzlichen kriminellen Handlungen – einschließt.

Doch auch Handwerksbetriebe sollten aufmerksam hinschauen, denn viele der im Gesetz formulierten Anforderungen – etwa im Bereich Risikoanalyse, Zutrittsmanagement oder Notfallvorsorge – entsprechen längst dem Stand der Technik. Wer eigene Server oder Produktions-IT betreibt, ist noch nicht gesetzlich verpflichtet, aber strategisch gut beraten, sich an diesen Standards zu orientieren. Denn die Angriffsfläche endet nicht an der Firewall. Sie beginnt oft an der ungesicherten Nebentür oder beim unbedarften Mitarbeiter, der nachts versehentlich ein Fenster offenläßt.

Der Autor

Christian Heppner ist Experte für strategisches Sicherheitsmanagement bei der SecCon Group GmbH mit Sitz in Unterschleißheim. Das Unternehmen bietet operative, spezialisierte Dienstleistungen für hochsensible Infrastrukturen und exponierte Personen. Zum Leistungsspektrum gehören zudem Risiko- und Schwachstellenanalysen, Sicherheitskonzepte und die Implementierung sicherheitsrelevanter Maßnahmen – auch in Zusammenarbeit mit Behörden und anderen Akteuren. Das auf KRITIS-Schutzkonzepte spezialisierte Unternehmen ist zudem Mitglied im Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI).

Sabotage und Vandalismus: übersehene Risiken

Während Cybergefahren medial präsent sind, bleiben andere reale Bedrohungen oft unter dem Radar. Sabotage, Vandalismus oder gezielte Einbrüche in IT- oder Lagerräume können binnen Minuten Schäden verursachen, die wochenlange Betriebsunterbrechungen nach sich ziehen. Besonders gefährdet sind Räume mit Servern, Elektroverteilungen oder sensibler Steuerungstechnik. Diese Bereiche sind häufig nur unzureichend gesichert, schlecht überwacht oder gar nicht dokumentiert. Dabei zeigen reale Vorfälle: Angreifer suchen gezielt nach Schwachstellen, und die sind nicht immer digital. Auch interne Konflikte, ehemalige Mitarbeiter oder externe Dienstleister können ein Risiko darstellen. >>

Autorenbild: SecCon Group

Was Betriebe jetzt tun sollten

Ein wirksames Schutzkonzept für Handwerksbetriebe beginnt mit einer nüchternen Analyse: Wo befinden sich kritische Systeme? Wer hat Zugang? Welche baulichen, organisatorischen und technischen Maßnahmen bestehen, und wie wirksam sind sie im Ernstfall? Hier empfiehlt sich ein pragmatisches Sicherheitskonzept mit vorangegangener Risikoanalyse: Dazu zählen klare Abläufe im Störfall, ein bewußter Umgang mit sensiblen Informationen und einfache organisatorische Maßnahmen, wie ein gezieltes Schlüsselmanagement oder Notfallpläne.

Durch Schulungen können Mitarbeiter sensibilisiert werden, und auch grundlegende technische Maßnahmen wie mechanische Sicherungen oder regelmäßige Datensicherungen tragen entscheidend zur Risikominimierung bei. Wer bereits in IT-Sicherheit investiert hat, sollte seine physische Infrastruktur nicht ausklammern, sonst bleibt ein entscheidendes Einfallstor offen.

FAZIT

Sicherheit ist heute mehr als ein Virenscanner. Im Zeitalter digital vernetzter Systeme wird physische Sicherheit zur Grundvoraussetzung für Resilienz. Auch Handwerksbetriebe müssen sich dieser Realität stellen. Nicht aus regulatorischem Zwang, sondern aus betrieblichem Eigeninteresse. Denn am Ende zählt nicht, was auf dem Papier sicher ist, sondern, was im Ernstfall tatsächlich schützt.

Noch Fragen?
https://www.seccon-group.de/de/