IT FÜR DEN MITTELSTAND

Mittelständler und Familienunternehmen sind längst ein genauso attraktives Ziel für Cyberkriminelle wie große Konzerne. Ihre Daten und die ihrer Kunden sind für Kriminelle nicht weniger interessant. Auch kleinere und mittlere Unternehmen (KMU) müssen daher ihre Sicherheitstechnologien und -strategien regelmäßig überdenken und anpassen. Experten helfen bei Fragen rund um die IT.

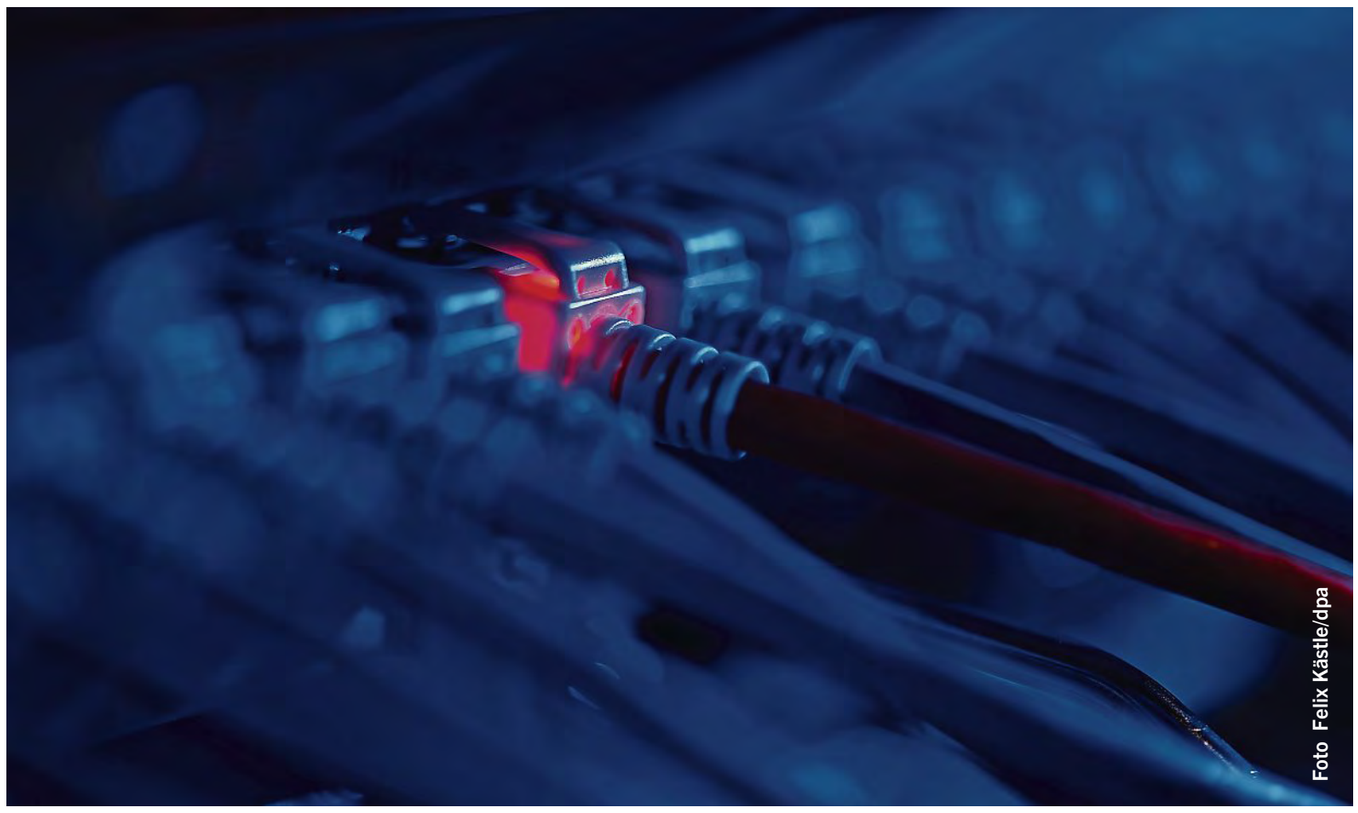


Foto Felix Kästle/dpa

Mittelstand nimmt IT-Sicherheit nicht ernst genug

Cyberangriffe. Hacker finden zunehmend bei kleineren Betrieben lohnende Ziele.

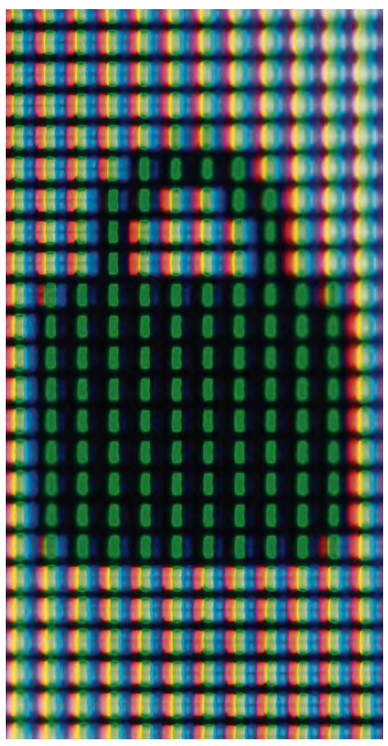
Die kleinen und mittelständischen Unternehmen (KMU) schludern bei der IT-Sicherheit. So deutlich wie der Gesamtverband der deutschen Versicherer (GDV) drücken es nur wenige aus. Der GDV-Cyberversicherungsexperte Peter Gauß geht noch weiter. „Es ist geradezu fahrlässig, wie der Mittelstand mit seiner IT-Sicherheit umgeht. Mittelständler sollten mindestens die einfachsten Sicherheitsregeln befolgen, denn immer mehr Betriebe sind von funktionierenden Computersystemen abhängig“, sagt er. Grund für diese eindeutige Aussage ist das Ergebnis einer Forsa-Umfrage unter 300 Entscheidern im Mittelstand im Frühjahr dieses Jahres, die der GDV in Auftrag gegeben hatte. Demnach haben etwa 80 Prozent der KMU Lücken in ihrer IT-Sicherheit.

Das nutzen Kriminelle immer häufiger aus. Es gelingt ihnen mit Angriffen, teilweise den ganzen Betrieb lahmzulegen, indem sie die Daten verschlüsseln, um anschließend Lösegeld zu erpressen. Oft geht es dann um die Existenz. So hat Cisco in der Umfrage „Cybersecurity Special Report Small and Midmarket Businesses“ unter 1800 Unternehmen in 26 Ländern ermittelt, dass bei jedem zweiten Sicherheitsvorfall der finanzielle Schaden bei mehr als 440 000 Euro lag. Zu den direkten Kosten kommt noch der Ausfall der unternehmenskritischen Systeme hinzu. Bei jedem vierten Unternehmen lag er bei über acht Stunden. „KMU sind längst ein genauso attraktives Ziel für Cyberkriminelle wie große Konzerne, da sie vor der Herausforderung stehen, das Sicherheitsniveau eines Konzerns mit wesentlich geringeren Mitteln erreichen zu müssen. Die Daten der Unternehmen und deren Kunden sind für Kriminelle nicht weniger interessant“, sagt Torsten Harengel, Leiter Security, Cisco Deutschland.

UNBEKANNTE TÄTER

Ein ernüchterndes Ergebnis hat auch das Beratungsunternehmen KPMG in der Studie „e-Crime in der deutschen Wirtschaft 2019“ veröffentlicht. Demnach wissen fünf von sechs Unternehmen nicht, wer hinter dem Cyberangriff auf die eigene Firma steckte. „Es ist eine der größten Herausforderungen für die Unternehmen, dass Täter kaum identifiziert werden können. Das muss wachrütteln“, sagt KPMG-Partner Michael Sauermann, Leiter Forensic Technology Deutschland, und ergänzt: „Unternehmen werden verstärkt über verschiedene Angriffsvektoren attackiert und müssen sich besser auf alle Angriffsszenarien vorbereiten.“

Eine der häufigsten Hackermethoden sind sogenannte Ransomware-Angriffe, die auch als Verschlüsselungs-Trojaner bekannt sind und zumeist den bereits erwähnten Erpressungsversuch zur Folge haben. Dabei entwickeln sich die Methoden immer weiter. So lösen diese Angriffe nicht nur die Interaktion aus, sie bedienen sich auch der kompletten Kontaktliste des Opfers und versenden die Software weiter. Diese Angriffe sind darüber hinaus immer öfter professioneller Natur. „Hacking-Angriffe können im Darknet käuflich erworben werden. Von Ransomware-Attacken über Überlastungsangriffe bis hin zu sogenannten Advanced Persistent Threats einschließlich Datendiebstahl ist alles erhältlich“, sagt Sauermann.



Datendiebstahl. Foto: dpa/Lino Mirgeler

Ein großes Problem bleiben dabei die Mitarbeiter. Nach Aussage der KPMG Umfrage fehlt es ihnen in deutschen Unternehmen zu 83 Prozent am Verständnis für komplexe Technologien, um Verdachtsfälle effizient zu beurteilen. Da verwundert es nicht, wenn nach Angaben des GDV noch über 70 Prozent der Schadsoftware über E-Mails den Weg ins Unternehmen findet.

Ein weiterer Schwachpunkt ist eine gewisse Selbstüberschätzung. So stellte der GDV fest, dass acht von zehn Firmen der Meinung sind, gut geschützt zu sein. Sie blenden die Gefahr aus. Dabei sind sie sich gleichzeitig durchaus bewusst, dass das Cyberrisiko für mittelständische Unternehmen eher hoch beziehungsweise sehr hoch ist. Daher empfiehlt der GDV, die Gefahr nicht zu unterschätzen. Weitere Tipps des Versicherungsverbandes: Unternehmen sollten unbedingt starke Passwörter nutzen und die Daten richtig sichern.

Wer sich im Unternehmen unsicher ist, ob seine Sicherheitsmaßnahmen ausreichend sind, der hat mittlerweile viele Anlaufstellen. Die bekannteste dürfte das Bundesamt für Sicherheit in der Informationstechnik (BSI) sein. Es bezeichnet sich selbst als der zentrale IT-Sicherheitsdienstleister. So hat das Bundesamt mit dem IT-Grundschutz eine Methodik entwickelt, um die Informationssicherheit in Unternehmen, aber auch in Behörden und Institutionen zu erhöhen. Gleichzeitig bietet das BSI eine Sicherheitsberatung an und sorgt für eine grundlegende Ausbildung in diesem Umfeld. *Ralf Johanning*

» impressum

Produktion: STZW Sonderthemen
Anzeigen: Jürgen Maukner

Große Vorteile für kleine Firmen

Ratgeber. Es muss nicht immer die Maßanfertigung sein. Vorkonfigurierte Software erlaubt auch kleinen und mittleren Unternehmen, an der Automatisierungsrevolution zu partizipieren.

Thomas Jaspers nutzt seit drei Monaten io-key – eine sogenannte Sensor-to-Cloud-Lösung, mit der der Paderborner Kerzenfabrikant Sensordaten über Füllstände und Wassertemperaturen via Internet abrufen und steuern kann. Das IT-Paket, das der Automatisierungs- und Sensorexperte Autosen initiiert und gemeinsam mit der Software AG und zwei weiteren Firmen entwickelt hat, ist leicht zu installieren und zu handhaben, bedarf weder hoher Investitionen noch IT-Expertise. „Ich muss keine Software programmieren, keine Wartung vornehmen, keine Weiterentwicklung betreiben“, sagt Firmenchef Jaspers. „Das System einzusetzen, ist so einfach, wie einen Backofen anschalten.“

Grund: Die Lösung des westfälischen Mittelständlers ist vorkonfiguriert – von der Hardware über die Cloud-Umgebung bis zur Datenflatrate. PC-Veteranen erinnern sich an Zeiten, in denen man stundenlang damit beschäftigt war, einen Rechner oder Kopierer in Betrieb zu nehmen, weil Hardware, Treiber und Software umständlich konfiguriert werden mussten.

Das muss heute nicht mehr sein. Viele Anbieter haben gerade für kleinere Unternehmern voreingestellte Systeme. Software-AG-Technikchef Bernd Gross: „So können auch diese Betriebe an der Automatisierungsrevolution teilhaben.“ Statt eines zu großen Anzugs von der Stange oder einer teuren Maßanfertigung werden in Serie vorgefertigte Produkte mit standardisiertem Funktionsumfang genutzt, die sofort einsatzbar sind. Stichwort: Plug&Play. Ein einfaches Frontend macht die Selbstbedienung auch für IT-Laien simpel. IT-Profi Gross: „Self-Service ist der Trend.“

Als Pionier vorgefertigter IT-Lösungen gilt Microsoft mit Windows 95. SAP hat den Mittelstand als Zielgruppe dagegen relativ spät entdeckt. Beratungs- und Systemhäuser übernahmen es, die für Großunternehmen entwickelten „Anzüge“ auch für kleinere Firmen tragbar zu machen. Heute arbeiten viele Mittelständler beispielsweise mit ERP-Systemen von SAP.

Vorteile? Steffen Klinzmann von Telekom: „Wollen Firmen funktionsfähige Prozesse haben oder Daten einspielen, dann gelingt das dank Public Cloud äußerst rasch.“ Sein Unternehmen bietet vorkonfigurierte Lösungen als sogenannte Dynamic Services. „Anwender setzen auf Bewährtem auf, statt bei null zu starten. Und sie buchen nur so viel ERP-System, wie sie brauchen. Abgerechnet wird der tatsächliche Verbrauch.“

Ähnlich macht es auch Eset, Großanbieter von Sicherheitssoftware. Kleinen und mittleren Firmen wird empfohlen, auf Fachhändler mit Managed Services zu setzen. „So erhalten Kunden genau das Paket, das zu ihren Anforderungen und ihrem finanziellen Rahmen passt“, erläutert Eset-Vertriebsdirektor Maik Wetzel. Der Kunde muss auch kein IT-Fachmann sein. „Spezialisierte Partner beraten vor Projektstart, übernehmen die Installation und verwalten kontinuierlich die Infrastruktur.“

Von abgespeckten Versionen seiner Software hält der Marktführer nichts. „Der Handwerker mit wenigen Rechnern erhält in seinen Sicherheitslösungen dieselben Technologien wie Großunternehmen.“ Der Kleine profitiere vom Großen, „weil ihm die Erkennungsmechaniken gegen neuartige Cyberangriffe auf Konzerne später auch zugutekommen“, sagt Wetzel.

Auch SAS, Weltmarktführer bei Analytics-Systemen, bietet Mittelstandslösungen. „Kleine und mittelständische Betriebe sehen sich mit denselben Herausforderungen konfrontiert wie Großunternehmen“, betont Annette Green, Vice President bei SAS für Deutschland, Österreich und die Schweiz. Auch sie stellten sich die Fragen: „Wie lassen sich aus vorliegenden Daten wichtige Informationen gewinnen, wie kann das Kundenerlebnis verbessert, wie die Mitarbeiterprofitabilität verbessert werden. Und zwar mit weniger Ressourcen und knappen Budgets.“

Dafür hat SAS das Produkt On-Demand-Analytics entwickelt, das vor Ort, via Cloud oder als Software as a Service bereitgestellt wird. Annette Green: „So kann jeder Betrieb, unabhängig von Größe und Branche, die Suche nach wichtigen Informationen unkompliziert und günstig beginnen.“ Die Umstellung von einer Desktop- auf eine Serverlizenz sei problemlos. *Jürgen Hoffmann*

Flexibel und effizient durch die Wolke

Cloud-Lösungen. Betriebe müssen gut überlegen, welchen Anbieter sie wählen wollen.

Mit Cloud Computing lassen sich auch in kleineren Betrieben viele Arbeitsabläufe vereinfachen. Aber was lagert man in die Daten-Wolke aus? „Ich halte es für sinnvoll, in die Cloud alle Systeme auszulagern, die ein Unternehmen standortübergreifend zur Verfügung stellen will“, sagt Stefan Patzelt, Innovations-Manager bei Systemintegrator Ostertag DeTeWe. Was liegt auf stationären Servern, das überall im Unternehmen gebraucht wird? Dazu gehören oft Office-Programmen, ERP-Systeme und Telefonie-Lösungen. „Der Cloud-Gedanke ist ja das Teilen. Wenn man das clever macht, werden Tools und Experten besser ausgelastet, Kosten zum Teil deutlich gesenkt.“

Dies seien auch Argumente für Betriebe, die von ihrer bisherigen analogen oder ISDN-Telefonanlage auf ein IT-strukturiertes System umsteigen wollen. Schlagwort: All-IP. Die Telefonanschlüsse sind hierbei an das Breitband gekoppelt. Dadurch sind mehr Funktionalitäten möglich, die Kapazität ist nicht mehr durch die Anzahl der Gesprächskanäle begrenzt, und die Grundgebühren für ISDN-Anschlüsse entfallen. Patzelt: „Cloud-Lösungen ermöglichen eine lineare Skalierbarkeit.“ Auch steige die Flexibilität. „Man kann Mitarbeiter variabel mit zusätzlichen Funktionen wie Fax, Video oder einer App für das Mobiltelefon ausstatten, etwa in saisonalen Peak-Phasen einen Buchhalter oder Einkäufer zu einem Callcenter-Agenten auf Zeit machen.“

MEHR EFFIZIENZ

Laut einer Untersuchung von Kaspersky Lab nutzen Firmen mit bis zu 249 Mitarbeitern beim Cloud Computing am häufigsten Software-as-a-Service-Anwendungen (73 Prozent). Sie versprechen sich davon Kostenreduktion, mehr Effizienz und Flexibilität für ihre Mitarbeiter. Zu den beliebtesten Anwendungen zählen E-Mail- und Speicher-Anwendungen, Collaboration- sowie Finanz- und Buchhaltungs-Services. Das bestätigt Arash Kaffamanesh, Geschäftsführer der Kölner Firma Clouds Sky. Gleichzeitig nehme bei kleineren Unternehmen, Vereinen, Clubs und anderen Organisationen die Skepsis gegenüber der Wolke als Datenverarbeitungsplatz ab. „Wir beobachten, dass viele Kunden für die Speicherung personenbezogener Daten zwar noch ihren stationären Server verwenden, für deren Verarbeitung aber durchaus Cloud Computing nutzen. Das wird klar getrennt.“

Was gehört in die Cloud, und was nicht? Foto: Adobe Stock/BillionPhotos.com

Nicht unbedingt in die Wolke auslagern würde Patzelt „unternehmenskritische Systeme“. Welche das sind, müsse jeder Betrieb für sich identifizieren. So manches produzierende Unternehmen beispielsweise entscheide sich, die digitale Steuerung ihrer Maschinen und Anlagen im eigenen Haus zu behalten. Er empfiehlt, Cloud-Computing-Anbieter auf die Sicherheit hin genau anzuschauen. „Stehen die Server in Deutschland, ist die verwendete Software ‚Made in Germany‘ und ist die Architektur georedundant, also mindestens an zwei oder drei unterschiedlichen Orten vorhanden?“ Kaffamanesh berichtet von Providern, deren Cloud-Server zwar in Deutschland stehen, Back-ups aber an Orten gelagert haben, auf die sich auch Unbefugte Zugriff verschaffen können. Sein Tipp: „Daten nur verschlüsselt ablegen.“ *Jürgen Hoffmann*