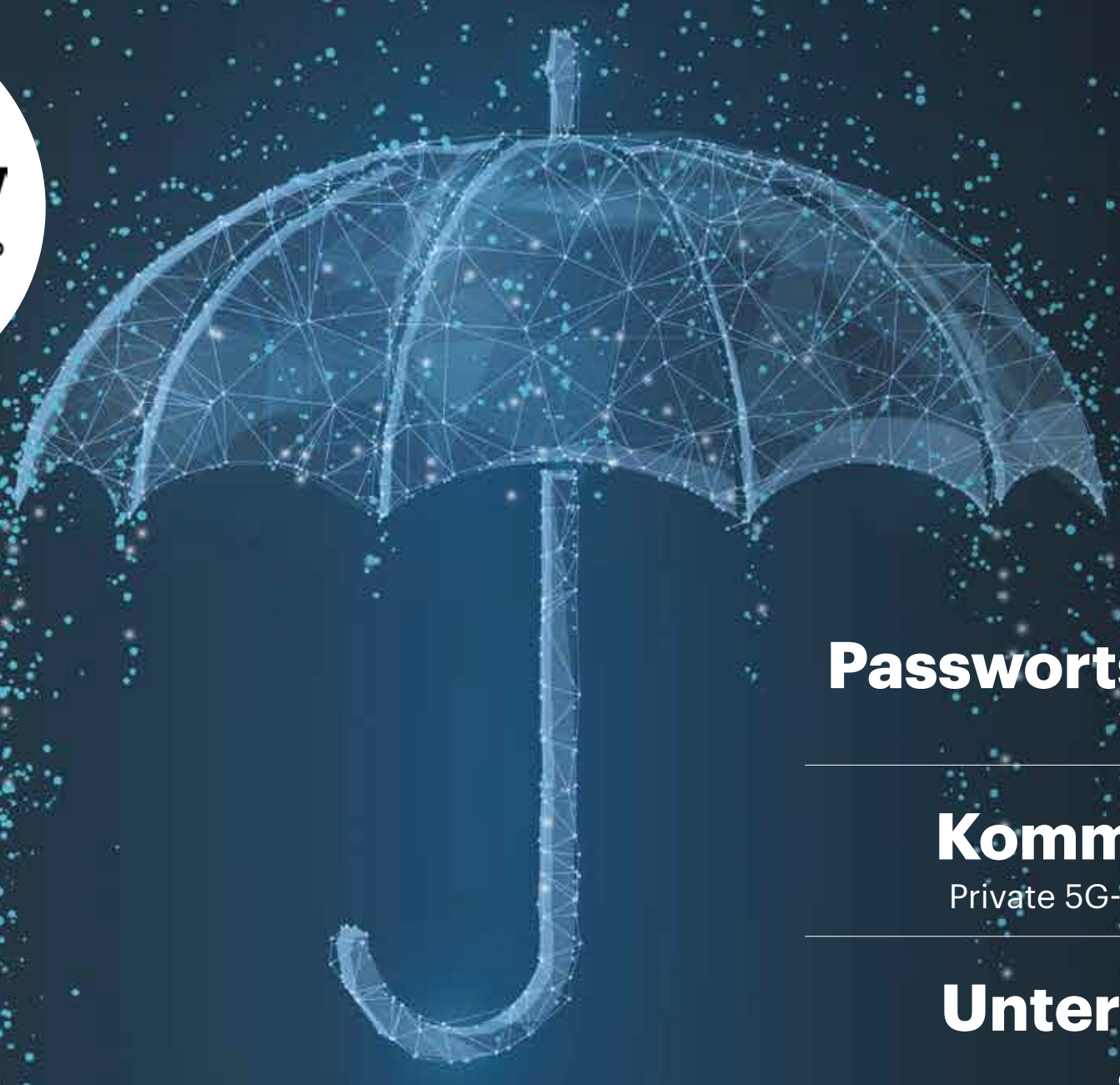
EINE PUBLIKATION VON SMART MEDIA

SEP '22

FOKUS SICHERHEIT

smart media agency



Passwortsicherheit
Worauf zu achten ist

Kommunikation
Private 5G-Netze bieten Schutz

Unternehmens-sicherheit
Nachhaltige Sicherheit fördern

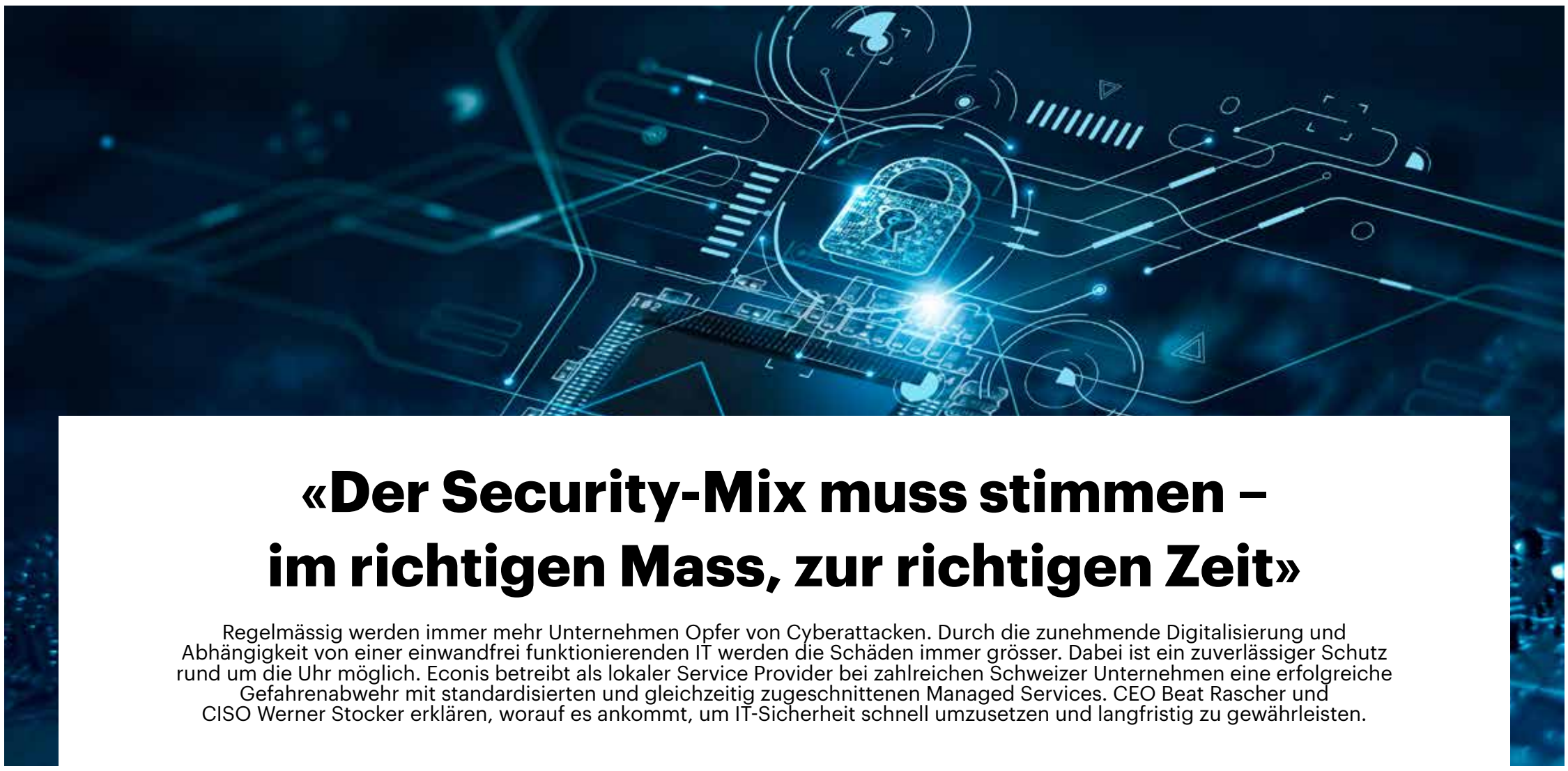
Interview

Florian Schütz

Delegierter des Bundes für Cybersicherheit

«Cybersicherheit muss auf Geschäftsleitungsebene thematisiert werden.»

Lesen Sie mehr auf fokus.swiss



«Der Security-Mix muss stimmen – im richtigen Mass, zur richtigen Zeit»

Regelmässig werden immer mehr Unternehmen Opfer von Cyberattacken. Durch die zunehmende Digitalisierung und Abhängigkeit von einer einwandfrei funktionierenden IT werden die Schäden immer grösser. Dabei ist ein zuverlässiger Schutz rund um die Uhr möglich. Econis betreibt als lokaler Service Provider bei zahlreichen Schweizer Unternehmen eine erfolgreiche Gefahrenabwehr mit standardisierten und gleichzeitig zugeschnittenen Managed Services. CEO Beat Rascher und CISO Werner Stocker erklären, worauf es ankommt, um IT-Sicherheit schnell umzusetzen und langfristig zu gewährleisten.

Beat Rascher
CEO Econis AG

Werner Stocker
CISO Econis AG

Beat Rascher, Werner Stocker, worin bestehen die Herausforderungen, wenn ein Unternehmen seine IT schützen will?
Beat Rascher: Viele Unternehmen denken beim Schutz vor Cyberangriffen zuerst an Ransomware. Dieser Ansatz ist nicht falsch, er ist jedoch ein Entscheid aus dem Bauchgefühl heraus – oder aus dem, was gerade in den Medien als kritisch angeschaut wird. Das hinterlässt blinde Flecken, da Informationssicherheitsrisiken an vielen Orten lauern.

Werner Stocker: Die grösste Herausforderung für die Unternehmens-IT ist, die Informationssicherheit in seiner Gänze als Prozess im Griff zu haben. Damit gelangt man von reaktiver Sicherheit, wo nur auf Ereignisse reagiert wird, in eine proaktive Sicherheit. Mittel- und langfristig ist man so zusätzlich auf die sich verändernde Sicherheitslandschaft vorbereitet.

Wie sieht eine zuverlässige 360-Grad-Sicherheitsarchitektur aus?
Werner Stocker: Sicherheit ist ein Prozess und die Architektur wird in regelmässigen Zyklen an die sich verändernden Rahmenbedingungen angepasst. Hierfür ist ein sauberes Inventar aller wichtigen Geschäftsanwendungen und deren Daten notwendig, die sogenannten Assets. Diese Assets werden bezüglich deren Sensitivität eingestuft und anschliessend in ein strukturiertes Konzept integriert, um diese gemäss deren Sensitivität individuell zu schützen. Eine zuverlässige Sicherheitsarchitektur besteht darin, genau diesen Spagat aus individuellem Schutz und Wirtschaftlichkeit über wenige standardisierte, sich ergänzende Komponenten zu erreichen.

Sie setzen einen wichtigen Fokus auf das Business-Continuity-Management. Was gilt es hier zu beachten?
Beat Rascher: IT ist mittlerweile die Grundlage aller Geschäftsprozesse geworden. Das bedeutet auch, dass ein längerer Ausfall der IT die Existenz von Firmen gefährdet. Beim Business-Continuity-Management geht es darum, alle Vorfälle zu identifizieren, welche den IT-Betrieb gefährden können und entsprechende vorbereitende Massnahmen zu treffen. Dies hilft, um beispielsweise bei grösseren Ausfällen über ein Backup-Rechenzentrum den Betrieb wiederherzustellen oder rasch auf Cyberangriffe reagieren zu können, um Schäden zu minimieren. Oft wird jedoch aus Kosten- und Ressourcengründen auf regelmässige Tests verzichtet. Diese Tests sind jedoch wichtig, um über deren Resultate Optimierungsmassnahmen zur Verbesserung der betrieblichen Stabilität einzuleiten. Business-Continuity-Management ist deshalb eine lohnenswerte Investition in die Zukunft zur Sicherstellung des Geschäftsbetriebes.

Wie unterstützen Sie Ihre Kunden bei der Asset Security & Compliance?
Werner Stocker: Die Kernkompetenz der Econis ist die Sicherheit als Prozess gemäss der ISO/IEC 27001-Zertifizierung. Dies bedingt, dass die Sensitivität aller wichtigen Kundenanwendungen und deren Daten bezüglich Vertraulichkeit (wer darf was sehen), Integrität (bis zu welchem Zeitpunkt in der Vergangenheit dürfen Daten verloren gehen), Verbindlichkeit (wie viele Jahre sind Daten rechtlich relevant) und Verfügbarkeit (wie lange dürfen Daten und Prozesse maximal ausfallen) bekannt sind. Dies wird damit angereichert, welche Regulatorien oder branchenspezifischen Bestimmungen jeweils vorliegen. Econis begegnet dabei den Kunden auf Augenhöhe und begleitet sie proaktiv bei der Erfüllung des IT-Grundschutzes inklusive der notwendigen Datenschutzprozesse. Das geht über das Vorfallsmanagement auch bis in das Business Continuity Management hinein.

Ein wichtiger Punkt ist bei Ihnen die Datenklassifikation. Da zucken manche Unternehmen immer noch mit den Schultern, weil sie nicht wissen, wie sie konkret mit welchen Daten umgehen sollen. Wie können Sie hier helfen?
Beat Rascher: Econis führt Kunden ohne Datenklassifikation auf einfache Weise in dieses Thema ein und zeigt die Vorteile daraus auf. Dies geschieht über die jährlichen Review-Prozesse für die an Econis ausgelagerten Managed Services. Wenn ein Kunde bereits eine Datenklassifikation hat, wird diese einfach gemappt, damit beide Seiten vom selben sprechen und die richtigen Massnahmen ergreifen können.

Werner Stocker: Econis kann hierbei als Leading by Example nicht nur helfen, diese Datenklassifikation sauber zu definieren, sondern auch technisch umzusetzen. Es können neben den Geschäftsanwendungen und Daten auch unstrukturierte Daten wie beispielsweise E-Mail und Office eingestuft und mit Sicherheitsprozessen belegt werden. Beispielsweise kann so verhindert werden, dass sensible Daten die Firma verlassen. Wichtig ist, dass hier pragmatisch an die Sache herangegangen wird, nach dem Prinzip «so viel wie nötig». Mit Econis können sich Kunden auf ihre Kerngeschäfte konzentrieren und haben mehr Zeit für das Wesentliche.

Im Econis-Security-Monitoring wollen Sie Cyber Security sichtbar machen. Wie werden dabei Angriffe von aussen leichter oder schneller erkannt?
Werner Stocker: Systeme und Anwendungen protokollieren alle Tätigkeiten. Darin verstecken sich oft auch Angriffe oder unerwünschte Aktivitäten. Über eine zentrale Sammlung und Auswertung in einem Security Operation Center kann die berühmte Nadel im Heuhaufen sichtbar gemacht werden. Zusammen mit strukturierten Vorfallshandbüchern werden so Angriffe effizient eingedämmt und grössere Schäden verhindert. Ein Security Operation Center kann aber nicht nur monitoren, sondern in einer weiteren Ausbaustufe auch schwerwiegende Angriffe automatisiert abwehren und damit grössere Ausfälle oder Datenabflüsse verhindern.

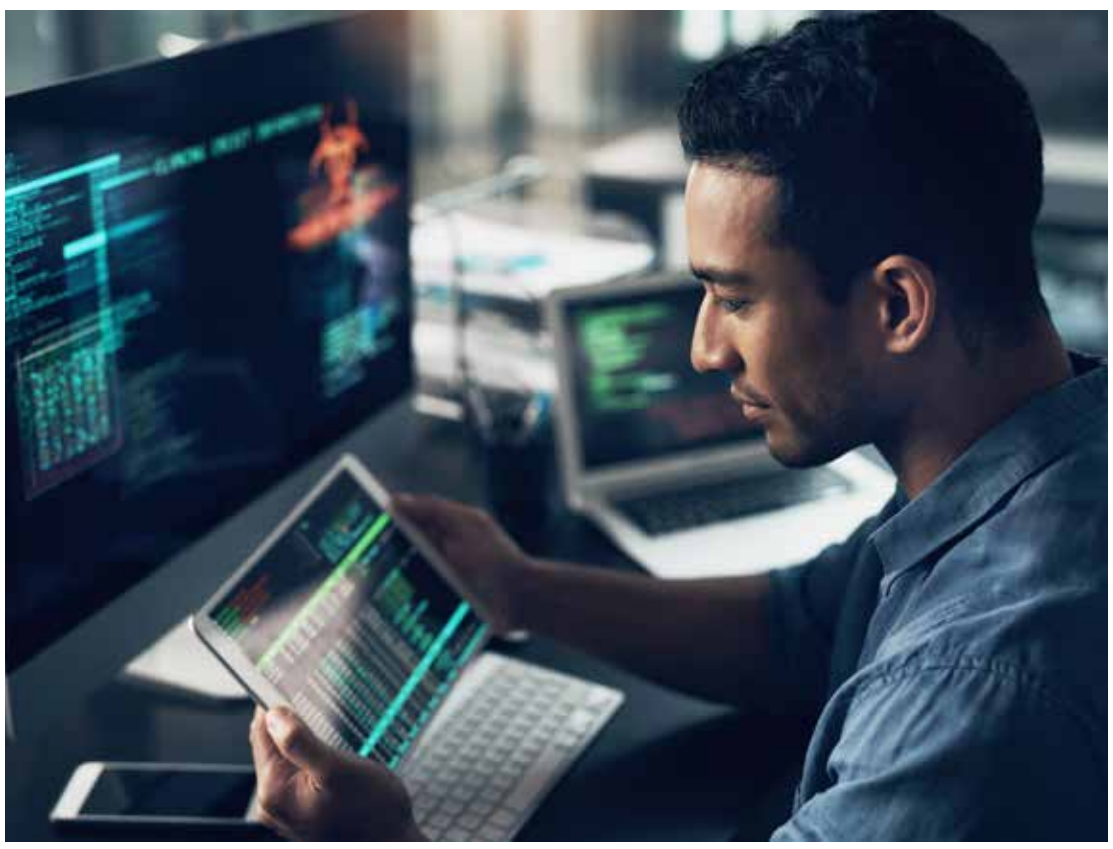
Sie schauen sich im sogenannten Vulnerability Management auch an, wo genau in Soft- und Hardware-Komponenten Schwachstellen liegen. Wird in Unternehmen zu wenig ganzheitlich auf Sicherheit gesetzt?
Werner Stocker: Die Kunst des Vulnerability Managements ist es, zu wissen, welche Anwendungen und Komponenten im Einsatz sind und ob diese verwundbar sind gegenüber Angriffen. Man muss deshalb ein vollständiges Inventar aller Anwendungen haben und wissen, welche Schwachstellen auf diese wirken. Hierüber legt man dann einen risikooptimierten Prozess, um Probleme zu beheben. Dabei werden kritische Schwachstellen priorisiert und entsprechend rasch behoben. Häufig wissen Unternehmen gar nicht, wo sie verwundbar sind. Econis bietet das Vulnerability Management für alle seine Managed Services an und kann den Kunden auch bei selbst- oder fremdverwalteten Anwendungen beim Tracking und Reporting von Schwachstellen unterstützen. Dieser Prozess wird technisch unterstützt, um menschliche Fehler ausschliessen zu können.

Was können Sie zusätzlich in Ihren Cyber-Security-Workshops und -Trainings vermitteln?
Beat Rascher: Econis hat aufgrund seiner Zertifizierung einen umfassenden Sicherheitsprozess etabliert. Wir bieten einmalige oder wiederkehrende Sicherheits-Beurteilungen in zwei Stufen an. In der einfachen Form wird auf Cyber-Security fokussiert. In der umfassenderen Form erfolgt eine vollständige Analyse gemäss ISO/IEC27001 und 2. Hierbei berät Econis bei der Optimierung der Informationssicherheit, unabhängig von den eingesetzten Massnahmen. Wir können dazu auf einen jahrelangen Erfahrungsschatz über verschiedenste Branchen zurückgreifen. Auch hier gilt es, über einen pragmatischen Ansatz rasch eine Visibilität zu erreichen, damit der Kunde seine Ressourcen optimal und umfassend auf die wichtigen Themen fokussieren kann. Daneben bieten wir eine auf den Kunden abgestimmte fortlaufende Sensibilisierung der Mitarbeitenden an. Dies geschieht über ein Web-Based-Awareness-Training und kann die Effektivität über simulierte Phishing-Angriffe auch regelmässig überprüfen.

Weitere Informationen unter
www.econis.ch

Interview **Rüdiger Schmidt-Sodingen**

> **«Die Kernkompetenz der Econis ist die Sicherheit als Prozess gemäss der ISO/IEC 27001-Zertifizierung.**



ECONIS
IT with passion