«Kleine Betriebe sind häufig verletzlicher»

6. Juni 2026 - **Informationssicherheit ist für viele Organisationen zentral. Durch den Einsatz von KI verändern sich Risikoprofile fundamental. Auditor Matthias Reetz zeigt, wie KI und Informationssicherheit gemeinsam gedacht und wirksam umgesetzt werden.**

Herr Reetz, Sie auditieren seit vielen Jahren Organisationen in unterschiedlichen Branchen. Wie hat sich die Risikolage in der Informationssicherheit entwickelt?
Matthias Reetz: Sie hat sich deutlich verschärft. Unternehmen sind heute stärker vernetzt, nutzen Cloud-Dienste und arbeiten enger mit externen Partnern zusammen. Dadurch hat sich auch das Bedrohungsspektrum erweitert. Gleichzeitig beobachten wir eine zunehmende Professionalisierung der Angreifer. Sie gehen gezielter vor, sind gut organisiert und meist wirtschaftlich motiviert.

Wird die Bedrohungslage Ihrer Erfahrung nach immer realistisch eingeschätzt?
Nein, nicht immer.

Inwiefern nicht?
Gerade kleinere und mittlere Organisationen denken oft: Wir sind doch zu klein, um interessant zu sein. In der

Realität unterscheiden automatisierte Angriffe aber nicht nach Unternehmensgrösse, und gerade kleinere Betriebe sind aufgrund knapper Ressourcen häufig verletzlicher.

Viele Organisationen reagieren auf diese verschärfte Lage mit einem Informationssicherheits-Managementsystem (ISMS) nach der ISO/IEC 27001. Welchen Nutzen bringt die Norm?
Sie hilft Organisationen, Informationssicherheit systematisch zu steuern, statt nur punktuell auf Vorfälle zu reagieren. Risiken werden strukturiert analysiert und darauf abgestimmte Schutzmassnahmen festgelegt.

Wie wirkt sich das im Arbeitsalltag aus?
Es entstehen klare Verantwortlichkeiten und nachvollziehbare Prozesse, und es gibt deutlich weniger Ad-hoc-Entscheidungen. Gleichzeitig verbessern Unternehmen ihre Fähigkeit, auf Sicherheitsvorfälle und neue Anforderungen von Kunden oder Behörden zu reagieren.

Parallel dazu hält KI Einzug in Geschäftsprozesse. Entstehen auch dadurch neue Risiken?
Auf jeden Fall, und zwar entlang des gesamten Daten- und Entscheidungszyklus, etwa wenn sensible Daten in KI-Tools eingegeben werden oder Entscheidungen auf intransparenten Modellen basieren. Auch Abhängigkeiten von einzelnen Technologieanbietern können problematisch werden, etwa wenn zentrale Geschäftsprozesse auf deren Plattformen laufen. Und wenn Mitarbeitende KI-Tools eigenständig nutzen, besteht die Gefahr, dass vertrauliche Informationen nach aussen gelangen oder Ergebnisse ungeprüft in Entscheidungen einfliessen.

Mit der ISO/IEC 42001 gibt es eine spezifische Norm für das Management von KI. Was ist ihr konkreter Nutzen für Anwenderinnen und Anwender?
Sie beschreibt, wie Organisationen den Einsatz von KI planen, steuern und kontinuierlich verbessern können. Im Mittelpunkt stehen dabei Governance, Risikobeurteilung, Transparenz und der Umgang mit Datenschutz- und Sicherheits- sowie ethischen Fragen.

Auf den ersten Blick behandeln die ISO/IEC 27001 und ISO/IEC 42001 zwei getrennte Themen. Sind sie in der Praxis verbunden?
Ja. Viele Elemente wie Risikomanagement, Schulungen oder interne Audits lassen sich sogar gemeinsam nutzen.

Schweizerische Vereinigung für Qualitäts- und -Management-Systeme
Die Schweizerische Vereinigung für Qualitäts- und Management-Systeme ist die führende Zertifizierungsstelle für ISO-Managementsysteme in der Schweiz. Sie ist eine Not-for-Profit-Organisation mit über 50 Mitgliederorganisationen aus der Schweizer Wirtschaft sowie weiteren wichtigen Akteuren aus öffentlicher Verwaltung, Wissenschaft und Zivilgesellschaft. Darunter auch Swico.
Wo liegen die grössten Herausforderungen bei diesem integrierten Vorgehen?
Meist weniger in der Technik als in der Organisation.

Was heisst das?
Informationssicherheit und KI lassen sich nicht isoliert in der IT lösen, sondern müssen als Querschnittsthemen über Fachbereiche, Compliance, Datenschutz und Management hinweg verankert werden. Gleichzeitig verlaufen KI-Projekte oft sehr dynamisch, während Managementsysteme auf Stabilität und Nachvollziehbarkeit angelegt sind. Hier braucht es die richtige Balance zwischen Agilität und klarer Steuerung.

Welchen Nutzen haben Organisationen davon?

Mehr Transparenz und bessere Steuerbarkeit. Unternehmen sehen klarer, wo Informationen und KI eingesetzt werden, welche Risiken bestehen und wie sie adressiert werden. Zudem entsteht eine belastbare Grundlage für Nachweise gegenüber Kundinnen, Auftraggebern und Behörden.

Wie lässt sich ein solch integrierter Ansatz pragmatisch umsetzen?
Wichtig ist, klein anzufangen und vorhandene Strukturen zu nutzen. Das kann zum Beispiel ein bestehendes Qualitätsmanagementsystem sein. Der Umfang des Managementsystems sollte zum Reifegrad der Organisation passen und schrittweise erweitert werden.