Zu viele Normen für die Informationssicherheit: Die Wahlkrise

von Andreas Wisler

IT-Standards spielen in der heutigen komplexen Welt eine entscheidende Rolle. Sie führen uns an, sorgen für Struktur und bieten eine gesteigerte Schutzgarantie. Aber was geschieht, wenn ein Segen zum Fluch wird? Eine schiere Überflutung mit Standards droht uns zu ertränken, anstatt uns zu helfen – genau das erleben wir derzeit im IT-Sicherheitsbereich.

DIE FLUT DER STANDARDS

Es existieren zahlreiche Normen, Standards und Frameworks, die die Behauptung vertreten, dass die Sicherheit von Informationen gewährleistet ist. Die Liste umfasst eine Vielzahl von Standards, darunter ISO/IEC 27001, NIST und COBIT sowie CIS Controls und PCI-DSS. Erst kürzlich ist die DIN SPEC 27076 – IT-Sicherheitsberatung für KMU erschienen. Jeder dieser Standards weist seine eigenen Schwerpunkte, Anwendungsbereiche und spezifischen Anforderungen auf.

Das Überangebot an Normen kann eine Paralyse verursachen. Unternehmen müssen sich die schwierige Frage stellen, welcher Standard für sie am besten passt. Vielfalt kann theoretisch von Nutzen sein, führt aber in der Realität häufig zu Verwirrung und Unsicherheit.

DIE GEFAHR DER ÜBERKOMPLEXITÄT

Wenn Unternehmen mehrere Normen gleichzeitig umsetzen wollen, nimmt die Komplexität exponentiell zu. Die Terminologien, Dokumentationsanforderungen und Kontrollen für jeden Standard sind individuell. Das Resultat? Ein undurchdringlicher Dschungel von Richtlinien, mit dem man sich kaum auseinandersetzen kann.

Nicht selten kommt es aufgrund dieser Komplexität vor, dass Sicherheitsmassnahmen nur teilweise realisiert werden. Managementteams verlieren den Überblick, Mitarbeiter sind überlastet und die tatsächlichen Sicherheitsziele werden vernachlässigt. Ein gefährlicher Zustand ist, dass der Verwaltungsaufwand die eigentliche Sicherheitsarbeit überlagert.

DER RUF NACH KONSOLIDIERUNG

Wir brauchen dringend eine Festigung der Standards. Darüber, welche Normen für welche Anwendungsfälle am besten geeignet sind, sollte sich gemeinsam verständigt werden. Ein bedeutender Fortschritt wäre eine einheitliche Struktur, die Unternehmen die Möglichkeit gibt, sich auf die wesentlichen Sicherheitsmassnahmen zu fokussieren.

Eine solche Vereinheitlichung könnte auch dazu beitragen, dass Sicherheitsstandards besser akzeptiert und verstanden werden. Wenn es eindeutige Richtlinien gibt, die sowohl für Fachleute als auch für Anwender verständlich sind, erhöht sich die Chance, dass diese Normen wirksam umgesetzt werden.

DER PRAGMATISCHE ANSATZ

Unternehmen sollten inzwischen eine pragmatische Vorgehensweise verfolgen. Sie sollten sich auf die Grundlagen der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – konzentrieren, statt sich in einem Meer von Standards zu verlieren. Ein auf Risiken basierender Ansatz, der die Bedürfnisse und Risiken des Unternehmens einbezieht, kann dazu beitragen, den Schwerpunkt zu behalten.

Ausserdem ist es von Bedeutung, die Angestellten fortlaufend zu schulen und zu sensibilisieren. Eine von allen Angestellten gepflegte Sicherheitskultur kann häufig mehr bewirken als nur eine geringe Einhaltung von Normen.

FAZIT

Paradoxerweise können zu viele Standards in der Informationssicherheit zu einer geringeren Sicherheit führen. Die Schwierigkeit liegt darin, den Überblick zu bewahren, ohne in der Flut verloren zu gehen. Eine effektive Informationssicherheit hängt von einer gezielten Auswahl und Anwendung der für das eigene Unternehmen relevanten Standards sowie einer ausgeprägten Sicherheitskultur ab.

Wir müssen den Kompass neu einstellen und den Kurs in eine Zukunft ausrichten, die sicher ist.

Andreas Wisler ist Inhaber und Senior Security Consultant der goSecurity AG ISO 27001, 27701 und 22301 Lead Auditor

www.goSecurity.ch | www.27001.blog | www.angriffslustig.ch