Bild: Pixabay

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

Zu viele Normen für die Informations-sicherheit

IT-Standards spielen in der heutigen komplexen Welt eine entscheidende Rolle, wie eine Art Kompass bieten sie eine Struktur und eine Erhöhung der Informationssicherheit. Aber was geschieht, wenn ein Segen zu einem Fluch wird? Eine schiere Überflutung an Standards droht uns zu ertränken, anstatt uns zu helfen – genau das erleben wir derzeit im IT-Sicherheitsbereich.

Es gibt unzählige Standards, Normen und Frameworks, die den Anspruch erheben, Informationssicherheit zu gewährleisten. Die Liste umfasst eine Vielzahl von Standards, darunter ISO/IEC 27001, NIST und COBIT sowie CIS Controls. Vor einigen Wochen ist zusätzlich die DIN SPEC 27076 – IT-Sicherheitsberatung für KMU erschienen. Jeder dieser Standards setzt einen eigenen Schwerpunkt, definiert einen Anwendungsbereich und verlangt spezifische Anforderungen.

ZUM AUTOR

Andreas Wisler, Dipl. Ing FH
goSecurity AG
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch

Inhalt der Normen/Standards

In diesem kurzen Artikel ist es nicht möglich, alle Details einer Norm festzuhalten. Schauen wir uns aber eine kurze Zusammenfassung an:

ISO/IEC 27001

Der Standard definiert die Anforderungen für die Einführung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines dokumentierten Informationssicherheits-Managementsystems (ISMS). Er umfasst die Verpflichtung an die Führung, einen umfassenden Risikomanagementprozess und Sicherheitskontrollen. Im Anhang sind 93 konkrete Massnahmen nach den Kategorien organisatorische Massnahmen, personelle Sicherheit, physische und umgebungsbezogene Sicherheit sowie technische Massnahmen unterteilt.

NIST Cyber Security Framework 2.0

Das NIST CSF ist ein strukturiertes Rahmenwerk für die Auswahl und Implementierung von Sicherheits- und Datenschutzkontrollen in Informationssystemen. Das Framework umfasst eine Liste von Sicherheitskontrollen, die nach Kategorien geordnet sind, wie zum Beispiel Zugriffskontrolle, Awareness- und Schulungsprogramme, Audits, Konfigurationsmanagement, Identitäts- und Authentifikationskontrollen, Incident Management, physische und umweltbezogene Sicherheit, Planung, Risikobewertungen, Kommunikationsschutz sowie System- und Informationsintegrität.

COBIT

COBIT (Control Objectives for Information and Related Technologies) ist ein Framework für das Management und die Governance von Unternehmens-IT, das von ISACA entwickelt wurde. Es basiert auf fünf Schlüsselprinzipien: Erfüllung der Stakeholder-Anforderungen; Abdeckung des gesamten Unternehmens; Anwendung eines integrierten Rahmens; Ermöglichung eines ganzheitlichen Ansatzes; Trennung von Governance und Management. Die Themen sind in fünf Domänen unterteilt: EDM (Evaluate, Direct, Monitor), APO (Align, Plan, Organize), BAI (Build, Acquire, Implement), DSS (Deliver, Service, Support), MEA (Monitor, Evaluate, Assess).

CIS Controls

Entwickelt wurden die Controls vom Center for Internet Security (CIS). Sie bieten eine priorisierte Liste von Sicherheitsmassnahmen, die helfen sollen, die häufigsten und gefährlichsten Cyberangriffe zu verhindern. Die CIS Controls sind in verschiedene Gruppen eingeteilt, um eine schrittweise Umsetzung zu erleichtern: Basic Controls wie Inventarisierung, Schwachstellen-Management, Berechtigungskontrollen; Foundational Controls wie Sicherheitskonfigurationen, Wartung und Überwachung, E-Mail und Webbrowser-Schutz, Malware-Abwehr, Netzwerk-Kontrollen, Backup und Wiederherstellung, Entwicklungssicherheit; Organizational Controls: Awareness, Umsetzung von Richtlinien und Verfahren, Kontrolle von Zugriffsrechten sowie Audits und Penetration Tests.

DIN SPEC 27076

Die DIN SPEC 27076 richtet sich an kleine und mittlere Unterneh-

men (KMU) und bietet einen Leitfaden für IT-Sicherheitsberatung. Ziel ist es, KMUs dabei zu unterstützen, angemessene IT-Sicherheitsmassnahmen zu ergreifen und so ihre Informationssicherheit zu verbessern. Die Spezifikation legt dabei besonderen Wert auf praxisnahe und umsetzbare Empfehlungen. Details dazu sind in der maschinenbau-Ausgabe vom Mai 2024 zu finden.

Dieses Überangebot an Normen kann eine Paralyse verursachen. Unternehmen müssen sich die schwierige Frage stellen, welcher Standard nun 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 ungewöhnlich kommt es aufgrund dieser Komplexität vor, dass Sicherheitsmassnahmen nur teilweise realisiert werden. Das Management verliert 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 Konsolidierung der Standards. Darüber, welche Normen für welche Anwendungsfälle am besten geeignet sind, sollte ein gemeinsames Verständnis erarbeitet 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 konzentrieren: Vertraulichkeit, Integrität und Verfügbarkeit. Statt sich in einem Meer von Standards zu verlieren. Ein auf Risiken basierender Ansatz, der die Anforderungen und Bedrohungen des Unternehmens berücksichtigt, 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 eine strenge Einhaltung von Normen.

Fazit

Paradoxerweise können zu viele Standards für die 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.