Cybersecurity mit System

Neue Version der ISO/IEC27001 stärkt Cybersecurity und Datenschutz

Der international etablierte Standard ISO/IEC 27001 ist die umfassendste Norm für Informationssicherheit. Sie wurde im Oktober 2022 in überarbeiteter Form veröffentlicht und enthält nun neue Maßnahmen für mehr Cybersicherheit und Datenschutz. Die wichtigsten Änderungen erfahren Sie hier und im Whitepaper des TÜV Süd.

Alexander Häußler

Gefährliche Zeiten: In unserer digital vernetzten und von Krisen geprägten Welt steigen die Anforderungen an die IT-Sicherheit rasant. Umso wichtiger wird es für Organisationen, sich mit einem Informationssicherheits-Managementsystem (ISMS) gegen diese Herausforderungen zu wappnen. Ein ISMS kann Organisationen jeder Größe helfen, sich gegen Cyberangriffe und andere böswillige Datenmanipulationen effektiv zu schützen und beugt dem Verlust sensibler Informationen vor. Die Norm ISO/IEC 27001 bietet einen detaillierten Rahmen für die Entwicklung, Einführung und Pflege eines solchen Managementsystems.

Die internationalen Standards ISO/IEC 27001 und ISO/IEC 27002 sind eng verknüpft und bilden die Basis für die Informationssicherheit in Unternehmen. Bei beiden Standards hatte es über einen längeren Zeitraum keine Überarbeitung gegeben. Angesichts der Geschwindigkeit, mit der sich die Cyberbedrohungslandschaft entwickelt, wurde es jedoch zunehmend notwendig, die vorgeschlagenen Maßnahmen (Controls) dem aktuellen Stand der Technik anzupassen. Nach einer Revision der ISO/IEC 27002 Anfang 2022, die maßgeblich für den Anhang der ISO/IEC 27001 ist, folgte auch für diese Norm eine Überarbeitung im Oktober 2022. Die neue ISO/IEC 27001:2022 löst damit die bisher geltende ISO/IEC 27001:2013 ab. Dadurch erhält sie eine lange erwartete Anpassung bei Maßnahmen zu IT-Sicherheit, Datenschutz sowie konkrete Maßnahmen zur Cloudsicherheit. Auch die Einbeziehung der obersten Führungsebene beim Aufbau einer cyber-resistenten Organisation wird in der neuen Version stärker betont.

Revision: Neue Maßnahmen und übersichtliche Struktur

Die ISO/IEC 27002:2022 hat eine neue, gut sichtbare und gebündelte Struktur, die das breite Spektrum der Informationssicherheit verdeutlicht. Die wichtigsten Änderun-

gen im Vergleich zur Vorgängerversion betreffen die im Anhang A definierten Maßnahmen (Controls). Diese wurden in vier Abschnitten neu gegliedert:

- Organisational Controls (37 Maßnahmen)
- People Controls (8 Maßnahmen)
- Physical Controls (14 Maßnahmen)
- Technological Controls (34 Maßnahmen).

Insgesamt hat sich die Anzahl der Maßnahmen gemäß ISO/IEC 27002:2022 von 114 auf 93 gegenüber der Vorgängerversion ISO/IEC 27002:2013 verringert. Wo nötig wurden die Maßnahmen aktualisiert, um den aktuellen Stand der Technik zu reflektieren. Außerdem wurden elf neue Maßnahmen eingeführt, die in der Vorgängerversion nicht ausdrücklich erwähnt sind:

- Threat Intelligence (Analyse von Cyberbedrohungen)
- Information Security for Use of Cloud Services (Informationssicherheit bei der Nutzung von Cloud-Diensten)
- ICT Readiness for Business Continuity (IKT-Bereitschaft für Business Continuity)
- Physical Security Monitoring (Überwachung der physischen Sicherheit)
- Configuration Management (Konfigurationsmanagement)
- Information Deletion (Löschung von Informationen)
- Data Masking (Maskierung von Daten)
- Data Leakage Prevention (Verhindern von Datenverlusten)
- Monitoring Activities (Überwachung von Aktivitäten)
- Web Filtering (Filtern schädlicher Websites)
- Secure Coding (Sichere Programmierung)

Verbessert: Cloud und Datenschutz

Die Zahl der Cloud-Anwendungen, die in Geschäftsprozesse, Systeme und Arbeitsabläufe integriert sind, nimmt zu, wodurch Angriffe auf Cloud-Prozesse für Hacker interessanter und lukrativer werden. Cloud-Lösungen und -Dienste, die in der Vergangenheit nur punktuell genutzt wurden, werden immer mehr direkt in die täglichen Geschäftsprozesse integriert. Sie sind damit ein kritisches Element für die Business Continuity von Unternehmen. Daher führt ISO/IEC 27001:2022 als eine der neuen Maßnahmen die „Informationssicherheit für die Nutzung von Cloud-Diensten" („Information security for use of cloud services") ein, um dem Trend zur Umstellung auf Cloud-Dienste Rechnung zu tragen. Das beinhaltet im Wesentlichen den Prozess, der für die Nutzung von Cloud-Diensten im Hinblick auf die Sicherheitsanforderungen eines Unternehmens erforderlich ist.

Die Vorschriften zum Datenschutz ändern sich weltweit, sodass große Cloud-Anbieter möglicherweise Vorschriften unterworfen werden, die nicht mit den Wünschen ihrer Kunden übereinstimmen. Je nach Land gelten beispielsweise unterschiedliche lokale Gesetze, die unter Umständen sogar Behörden Zugriff auf personenbezogene Daten gewähren. Ein weiterer Schwerpunkt der aktualisierten Norm ist daher der Datenschutz. Zwei neue Maßnahmen sind hier besonders erwähnenswert: „Data Leakage Prevention" und „Data Masking". Die Maskierung von Daten (im Gegensatz zur Verschlüsselung) ist keine direkte Anforderung der Datenschutz-Grundverordnung (DSGVO), kann jedoch einen guten Beitrag zur Pseudonymisierung liefern und stellt nun eine Maßnahme im Rahmen eines ISMS dar.

Bereits vor der Einführung eines ISMS muss analysiert werden, welche Informationen schützenswert sind. Diese Einschätzung basiert auf der Art der Information, Compliance-Regelungen und dem möglichen Schaden. Hierbei werden Vertraulichkeit aber auch Integrität und Verfügbarkeit der Daten betrachtet. Die Ergebnisse und die resultierenden Maßnahmen gilt es regelmäßig zu prüfen. Dieser Vorgang wird gemäß Plan-Do-Check-Act wiederholt, um Prozesse zu optimieren und diese an Änderungen anzupassen. ■

Vorteile einer ISO/IEC 27001-Zertifizierung

Organisationen, die ihr ISMS nach den Anforderungen von ISO/IEC 27001 zertifizieren lassen, profitieren von zahlreichen wichtigen Vorteilen.

Regulatorische Compliance
Ein ISO/IEC 27001-zertifiziertes ISMS kann einer Organisation helfen, gesetzliche und regulatorische Anforderungen unterschiedlicher Rechtsräume, sowie vertragliche Anforderungen für Geschäftsbeziehungen mit anderen Unternehmen zu erfüllen.

Systematischer Ansatz
ISO/IEC 27001 bietet einen formalen, systematischen Ansatz für die Informationssicherheit und erhöht das Schutzniveau für sensible und vertrauliche Informationen.

Reduzierte Risiken
Eine verbesserte Informationssicherheit kann Risiken reduzieren und dazu beitragen, die Auswirkungen von eintretenden Vorfällen möglichst gering zu halten.

Geringere Kosten
Eine ISO/IEC-Zertifizierung kann durch die Verringerung des Risikos von Sicherheitsvorfällen die mit der IT-Sicherheit verbundenen Gesamtkosten sowie die kostspieligen Folgekosten von Sicherheitsvorfällen deutlich reduzieren.

Wettbewerbsvorteil
Eine ISO/IEC 27001-Zertifizierung zeigt ein starkes Engagement für die Sicherheit von vertraulichen Informationen und kann einen bedeutenden Wettbewerbsvorteil bieten. Unternehmen erwarten von ihren Lieferanten zudem immer öfter ein nach ISO/IEC 27001 zertifiziertes ISMS.

Ein zertifiziertes Informationssicherheits-Managementsystem reduziert Risiken. Quelle: TÜV Süd © Hanser

INFORMATION & SERVICE

QUELLEN

Whitepaper zum Download:
www.tuvsud.com/whitepaper/iso-iec-27001

AUTOR

Alexander Häußler ist Global Product Performance Manager IT und Lead Auditor bei TÜV Süd für eine Vielzahl von IT-Sicherheitsstandards wie ISO/IEC 20000–1, ISO/IEC 27001 und die Erstellung von Nachweisen über angemessene IT-Sicherheit nach §8a BSIG.

KONTAKT

Alexander Häußler
Alexander.Haeussler@tuvsud.com