ISO 27008 – Leitlinien für die Bewertung von ISMS

Wer sich mit der Informationssicherheit auseinandersetzt, wird schnell auf die ISO 27001 oder den IT-Grundschutz des BSI (Deutsches Bundesamt für Sicherheit in der Informationstechnik) stossen. ISO 27001, wie auch der BSI 200-1, zeigt, was ein ISMS (Informationssicherheitsmanagementsystem) beinhalten muss. Jedoch werden keine Leitlinien zur Prüfung dieser Massnahmen aufgezeigt und damit die Frage, ob alle notwendigen Schritte korrekt umgesetzt sind, offengelassen. Genau an dieser Stelle setzt die ISO/IEC TS 27008:2019 an.

Bild: Pixabay

Da es keine Leitlinien zur Prüfung der ISMS gibt, wird die ISO/IEC TS 27008:2019 angewendet.

Die Norm bietet einen praxisnahen Leitfaden zur Überprüfung und Bewertung von Informationssicherheitskontrollen. Sie ist für Firmen aller Grössen und Branchen gedacht und bietet eine methodische Basis, um die Wirksamkeit und Angemessenheit von Sicherheitsmassnahmen nachvollziehbar zu prüfen. Besonders an dieser Norm ist, dass sie einen Ansatz mit methodischer Strenge und flexibler Anwendung vereint. Die Norm erkennt an, dass jede Firma ihre eigenen Rahmenbedingungen, Risiken und Ressourcen hat. Deshalb verzichtet sie auf starre Vorgaben und stattet Auditoren und ISMS-Verantwortliche mit einem Werkzeugset aus, mit dem sie ihre eigenen Massstäbe festlegen können, aber dennoch ein einheitliches Ergebnis erzielen.

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

Struktur der Norm

Nach einer kurzenz Einleitung und einigen Hintergrunddetails gibt es einen Überblick über den gesamten Prozess zur Bewertung von Informationssicherheitskontrollen. Es werden nicht nur technische Prüfungen, sondern auch die Prozesse, in denen die Kontrollen angewendet werden, berücksichtigt.

Die Norm macht einen Unterschied zwischen der eigentlichen Bewertung, den verwendeten Methoden und dem Ablauf der Kontrollbewertung. Sie umfasst somit den gesamten Prozess, von der Vorbereitung über die Durchführung bis zur Auswertung und dem Reporting. Mehrere Anhänge bieten konkrete Leitfäden zur Umsetzung. Ein besonderer Fokus liegt dabei auf Anhang B, der einen praxisnahen Leitfaden für technische Sicherheitsbewertungen bietet, sowie auf Anhang C, der die Bewertung von Cloud-Diensten behandelt.

Einstieg in die Bewertung von IS-Kontrollen

Die Bewertung von Informationssicherheitskontrollen ist ein wichtiger Bestandteil des gesamten Risikomanagements. Um Risiken zu managen, die nicht akzeptiert werden können, werden unter anderem Kontrollen durchgeführt. Ohne eine systematische Überprüfung ist es jedoch kaum möglich zu beurteilen, ob diese Massnahmen wirklich den gewünschten Erfolg bringen. Kontrollen müssen dabei zweckmässig sein, das heisst eine Kontrolle muss geeignet sein, das angestrebte Risiko zu behandeln. Eine Richtlinie für Passwörter ist sinnvoll, um unbefugten Zugriff zu verhindern, aber sie schützt nicht vor einem Ausfall des Rechenzentrums. Die Wirksamkeit bezieht sich darauf, ob die Kontrolle in der Praxis so funktioniert, wie es vorgesehen war. Eine Firewall-Regel mag auf dem Papier sinnvoll sein, doch wenn sie falsch konfiguriert ist, kann sie sogar gefährlich sein. Die Bewertung der Effizienz erfolgt schliesslich anhand der Frage, ob der Nutzen der Kontrolle im Verhältnis zum Aufwand steht. Niemand will Massnahmen, die zwar theoretisch perfekt schützen, aber den Geschäftsbetrieb lahmlegen oder unverhältnismässige Kosten verursachen.

Die Norm stellt klar, dass eine solide Informationsbasis das Fundament für Bewertungen sein muss. Dies umfasst alles von technischen Einzelheiten wie Systemkonfigurationen oder Logfiles bis hin zu organisatorischen Elementen wie Richtlinien, Rollenbeschreibungen und vergangenen Auditergebnissen. Um die Vorbereitung optimal zu nutzen, sammeln Prüfer deshalb so viele Informationen wie möglich. Sie reden mit den Verantwortlichen, werten frühere Prüfberichte und relevante Vorfälle aus und analysieren technische Dokumentationen. Es geht darum, ein klares Bild zu erhalten, bevor die eigentliche Überprüfung beginnt.

Hierbei ist der risikobasierte Ansatz wichtig. Die Norm empfiehlt, Kontrollen nicht immer gleich zu bewerten, sondern sie nach Priorität zu sortieren. Systeme und Kontrollen, deren Ausfall gravierende Folgen hätte, sollten besonders kritisch betrachtet werden. Umgekehrt können Bereiche mit geringerem Risiko mit weniger Aufwand kontrolliert werden. Es dreht sich also darum eine Balance zwischen Detailtiefe und Pragmatismus zu finden. Einerseits müssen Prüfungen genügend Substanz haben, um echte Schwachstellen zu erkennen; andererseits sollten sie vermeiden, in endlose Detailarbeit abzudriften, die den praktischen Nutzen mindert. Ein wichtiges Werkzeug dafür ist das vorgängige Erstellen von Bewertungschecklisten. Auch muss der Prüfer über die entsprechende Kompetenz verfügen, um die Kontrollen entsprechend durchzuführen.

Überprüfungsmethoden

Ein erster Schritt ist die Prozessanalyse. Es wird nicht direkt an den Kontrollen selbst angesetzt, sondern an den Prozessen. Beispielsweise wird betrachtet, wie das Incident Management strukturiert ist, welche Schritte bei einem sicherheitsrelevanten Ereignis geplant sind und wie die

Kommunikation im Ernstfall abläuft. Ein grosser Vorteil dieses Ansatzes ist, dass durch die Beobachtung des Prozessverlaufs die Effektivität der zugrundeliegenden Kontrollen bewertet werden kann. Ein funktionierender Prozess erzeugt Nachweise wie Protokolle, Alarmmeldungen oder Berichte, die belegen, dass die Kontrollen tatsächlich wirken.

Neben der Analyse der Prozesse werden auch klassische Prüfverfahren angewendet. Es wird überprüft, ob eine Kontrolle so existiert, wie sie dokumentiert ist, ob sie richtig konfiguriert wurde und ob sie den beabsichtigten Zweck erfüllt. Dies kann das Beobachten eines Backup-Vorgangs, das Überprüfen einer Firewall-Regel oder die Kontrolle physischer Sicherheitsmassnahmen wie Zutrittskontrollen umfassen.

Test- und Validierungstechniken liefern besonders aussagekräftige Ergebnisse. Sie gehen einen Schritt weiter, indem sie ein Prüfobjekt aktiv testen. Statt nur zu betrachten, ob eine Kontrolle vorhanden ist, wird evaluiert, ob sie in einer konkreten Situation zuverlässig reagiert. Das umfasst unter anderem Penetrationstests, bei denen versucht wird, in ein System einzudringen, oder Übungen zur Notfallbewältigung, die demonstrieren, ob ein Krisenplan wirklich funktioniert. Es ist wichtig, dass solche Tests sorgfältig geplant werden, weil sie den laufenden Betrieb beeinflussen können. Sie sind jedoch die wertvollsten Erkenntnisse, da sie das reale Verhalten einer Kontrolle sichtbar machen.

Ein Kapitel der Norm widmet sich den unterschiedlichen Testformen, die sich in ihrer Tiefe unterscheiden. Ein Blindtest zum Beispiel wird ohne Vorwissen über die Zielsysteme durchgeführt. Der Prüfer verhält sich wie ein Angreifer, der ausschliesslich auf öffentliche Informationen zugreifen kann. Ein Doppelblindtest hat noch eine weitere Ebene: Sogar die Firma ist im Unklaren darüber, wann und wie getestet wird. Das Ergebnis zeigt, wie gut eine Firma auf unerwartete Ereignisse reagieren kann.

Im Gegensatz dazu steht der Tandem-Test: Hier kennen die Prüfer und die Organisation alle Details von Anfang an und prüfen gemeinsam. Es dreht sich weniger um den Überraschungs-Effekt, sondern um eine detaillierte technische Analyse, die oft auch als interne Überprüfung dient. Dazwischen befinden sich Grey-Box-Tests. Der Prüfer verfügt über ein begrenztes Vorwissen und kann damit sowohl technische Schwächen als auch die Reaktionsfähigkeit der Firma überprüfen. Abschliessend wird in der Norm die Umkehrungsmethode beschrieben: Hierbei kennt der Prüfer das System sehr gut, während die Organisation nicht informiert ist, wann und wie die Prüfung stattfindet. Das ist vergleichbar mit einer Red-Team-Übung, die Angriffe in der Realität nachstellt und das Verteidigungsverhalten testet.

Neben diesen intensiven Testverfahren gibt es noch die Möglichkeit der Stichprobenprüfung. Sie ist dann sinnvoll, wenn es nicht möglich ist, alle Systeme oder Daten zu überprüfen. Es werden repräsentative oder besonders wichtige Bereiche ausgewählt, um Rückschlüsse auf das gesamte System zu bekommen. Die Herausforderung dabei ist es, die Stichproben so auszuwählen, dass sie die Realität bestmöglich widerspiegeln.

Alle diese Methoden lassen sich kombinieren. Es kann mit einer Prozessanalyse gestartet werden, um einen ersten Eindruck zu erhalten. Dieser wird mit Stichprobenprüfungen erweitert. Eine gründliche Bewertung sollte aber alle Schritte enthalten: die Prozessanalyse, die Prüfverfahren und umfassende Tests. Die gewählte Tiefe hängt vom Risiko, vom Umfang und von den Zielen ab.

Kontrollbewertungsprozess

Alles beginnt mit der Vorbereitung. Ohne eine klare Zielvorgabe und eine Planung läuft jede Bewertung Gefahr, sich in Details zu verlieren oder entscheidende Punkte zu übersehen. In dieser Phase wird bestimmt, welche Systeme und Kontrollen im Mittelpunkt stehen, welche Ressourcen benötigt werden und welche Rollen daran beteiligt sind. Auch die Kommunikation spielt eine entscheidende Rolle: Die Firma muss wissen, was sie erwartet, welche Informationen sie bereitstellen soll und wie der Austausch mit den Prüfern abläuft.

Als Nächstes wird die Planung der Bewertung angegangen. An dieser Stelle legen die Prüfer fest, welche Vorgehensweise sie konkret wählen wollen. Das beinhaltet die Auswahl der Überprüfungsverfahren, die am besten geeignet sind, um die jeweiligen Kontrollen zu prüfen. Die Norm hebt hervor, dass dies nicht schematisch erfolgen darf, sondern sollte immer risikobasiert erfolgen: Je kritischer eine Kontrolle ist, desto gründlicher muss sie geprüft werden.

Besonders interessant ist die Betonung des Kontexts. Eine Kontrolle ist nie isoliert; sie gehört immer zu einem grösseren System. Aus diesem Grund ist es wichtig, bei der Bewertung zu berücksichtigen, welche Prozesse und Abhängigkeiten existieren und wie die Kontrolle im Zusammenspiel mit anderen wirkt. Nur so kann realistisch beurteilt werden, ob sie wirklich den gewünschten Schutz bietet.

Als nächstes folgt die Durchführung der Bewertung. An dieser Stelle kommen die zuvor geplanten Methoden ins Spiel, sei es durch Prozessanalysen, Tests oder Stichproben. Es ist entscheidend, dass die Prüfer die Ergebnisse genau festhalten und dabei gleichzeitig den Schutz sensibler Daten gewährleisten. Das Ergebnis einer Prüfung kann erfüllt, teilweise erfüllt oder nicht erfüllt sein.

Danach erfolgt die Analyse und das Reporting. Hier ist besondere Vorsicht geboten: Die Ergebnisse müssen nicht nur richtig, sondern auch verständlich sein. Das Management benötigt eindeutige Antworten: Wo stehen wir? Welche Kontrollen sind effektiv? In welchen Bereichen sind wir schwach? Welche Risiken bestehen weiterhin, und welche Massnahmen sind sinnvoll?

Der Prozess endet jedoch nicht mit dem Bericht. Die Norm legt grossen Wert auf das Follow-up. Ohne Nachverfolgung verlieren Empfehlungen und Massnahmen ihre Wirkung. Eine Kontrolle, die als unzureichend bewertet wurde, bleibt ein Risiko, solange sie nicht verbessert oder durch eine andere ersetzt wird. Aus diesem Grund umfasst der Kontrollbewertungsprozess auch die Überwachung des Fortschritts, um sicherzustellen, dass Ergebnisse tatsächlich umgesetzt werden.

Anhänge

Der Anhang A zeigt, was die erste Informationsbeschaffung enthalten sollte. Er geht auf das Personalwesen, Richtlinien, Organisation, physische Sicherheit und das Incident Management ein.

In Anhang B ist für jeden Normpunkte der alten ISO 27001:2013 eine Kontroll-Frage abgebildet. Bei den technischen Kontrollen sind zusätzliche Informationen zu finden. Auch wenn inzwischen die 2022er-Ausgabe verfügbar ist, kann davon profitiert werden. Im Anhang der ISO 27002:2022 ist eine Mapping-Tabelle zwischen den alten und neuen Massnahmen abgebildet.

Was der Anhang B für die ISO 27001 ist, ist der Anhang C für die ISO 27017:2015, also der Kontrolle von Cloud-Diensten, speziell für Infrastructure as a Service. Es sind sehr detaillierte Informationen verfügbar, insbesondere zum Sicherheitsimplementierungsstandard. Im Mittelpunkt stehen Fragen wie: Sind die vereinbarten Sicherheitsmassnahmen des Providers tatsächlich umgesetzt? Werden Logs und Protokolle ausreichend bereitgestellt? Und wie können Kunden sicherstellen, dass ihre eigenen Pflichten im Zusammenspiel mit dem Cloud-Anbieter erfüllt werden?

Fazit

Die ISO/IEC TS 27008:2019 ist nicht einfach eine technische Spezifikation; sie bietet viel mehr. Mit dieser Norm wird eine wichtige Lücke geschlossen: Sie zeigt, wie Kontrollen nicht nur implementiert, sondern auch hinsichtlich ihrer Wirksamkeit bewertet werden können. Im Zusammenspiel mit den beiden Normen ISO 27001 und ISO 27002 können nicht nur die Massnahmen umgesetzt, sondern auch entsprechend geprüft werden.