# Informationssicherheit messen

**Wer misst, misst Mist. Diesen Satz lernte ich gleich zu meiner Ausbildung zum Elektroniker. Dies gilt nicht nur bei der Elektrotechnik, auch bei der Messung der Informationssicherheit ist es wichtig zu definieren, was gemessen wird, wie dies durchgeführt wird und wie die Ergebnisse zu interpretieren sind. Die ISO 27004 hilft, genau dies durchzuführen.**

Die Informationssicherheit zu messen, ist eine grosse Herausforderung. Welche Punkte gilt es zu messen? Wie kann sichergestellt werden, dass sich das ISMS wirklich weiterentwickelt und verbessert? Die ISO 27004 mit dem Titel «Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation» bietet eine Anleitung zur Beantwortung folgender Fragen:

- die Überwachung und Messung der Leistung der Informationssicherheit;
- die Überwachung und Messung der Wirksamkeit des ISMS einschliesslich seiner Prozesse und Kontrollen;
- die Analyse und Bewertung der Ergebnisse der Überwachung und Messung.

Die Norm ist in die Kapitel Gründe, Merkmale, Arten von Massnahmen und Abläufe unterteilt. Aber woher kommt die Anforderung, Informationssicherheit überhaupt zu messen? Dies ist in der ISO 27001:2013, Punkt 9.1 definiert. Die Organisation muss bestimmen:

a) was überwacht und gemessen werden muss, einschliesslich der Informationssicherheitsprozesse und Massnahmen;
b) die Methoden zur Überwachung, Messung, Analyse und Bewertung, sofern zutreffend, um gültige Ergebnisse sicherzustellen;
c) wann die Überwachung und Messung durchzuführen ist;
d) wer überwachen und messen muss;
e) wann die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind; und
f) wer diese Ergebnisse analysieren und bewerten muss.

Der Punkt a) wird in den Kapiteln 6.2 und 6.3, c) und e) im Kapitel 6.4, d) und f) in Kapitel 6.5 sowie b) in den Kapiteln 7, 8 und dem Anhang. Im Kapitel 5.4 geht die Norm darauf ein, welche Vorteile eine regelmässige Messung bringt. Es sind dies:

- Erhöhte Rechenschaftspflicht
- Verbesserte Informationssicherheitsleistung und ISMS-Prozesse
- Nachweis der Erfüllung von Anforderungen
- Unterstützung bei der Entscheidungsfindung

Doch was soll ich überwachen, um aussagekräftige Ergebnisse zu bekommen? Auch hier hilft die Norm weiter und zählt in Kapitel 6.2 einige, nicht abschliessende Punkte auf. Dies könnten beispielsweise sein:

- Stand der Implementierung von ISMS-Prozessen;
- Vorfälle von Incidents (technisch, wie auch Informationssicherheit);
- Korrekter Umgang mit Schwachstellen;
- Management der Konfigurationen;
- Sicherheitsbewusstsein der involvierten Personen;
- Zugriffskontrolle, Firewall und andere Ereignisprotokolle;
- Ergebnisse von Audits;
- Stand des Risikobewertungsprozesses und Behandlung dieser;
- Stand des BCMs;
- Physisches Sicherheitsmanagement; und
- Systemüberwachungen.

Diese Aufzählung entspricht den Anforderungen des Anhangs der ISO 27001. Dort sind 114 Controls in 14 Kapiteln aufgeführt (siehe dazu Maschinenbau 2018.4). Nun gilt es zu definieren, wann überwacht, gemessen, analysiert und bewertet werden soll (Kapitel 6.4) sowie wer überwacht, misst, analysiert und bewertet (Kapitel 6.5).

In Kapitel 7 werden Messungen der Leistung und der Effektivität erläutert. Leistungsmassnahmen können verwendet werden, um den Fortschritt bei der Implementierung von ISMS-Prozessen, zugehörigen Verfahren und spezifischen Sicherheitskontrollen nachzuweisen. Die Effektivitätsmassnahmen sollten verwendet werden, um die Wirksamkeit und die Auswirkungen zu beschreiben, die die Realisierungen der ISMS-Risikobehandlung und der ISMS-Kontrollen auf die Informationssicherheitsziele haben. Diese Massnahmen sollten verwendet werden, um festzustellen, ob die ISMS-Prozesse und Kontrollen der Informationssicherheit wie beabsichtigt funktionieren und die gewünschten Ergebnisse erzielen.

Das Kapitel beschreibt die Überwachung, Messung, Analyse und Bewertung und beinhaltet den folgenden Prozess:

a) Bedarf identifizieren;
b) Definieren der Massnahmen;
c) Verfahren zur Messung definieren;
d) überwachen und messen;
e) Analyse der Ergebnisse; und
f) die Leistung der Informationssicherheit und die Wirksamkeit des ISMS bewerten.

Der Bedarf lässt sich am einfachsten an den Anforderungen der Stakeholders auf das ISMS erarbeiten. Dies können die Interessierten Parteien, die Geschäftsstrategie des Unternehmens, die Vorgaben aus Richtlinien und Zielen sowie die Resultate aus Risiko-Analysen sein.

Die Messungen leiten sich aus dem Anwendungsbereich, der Firmen-Struktur, Firmenzielen, rechtlichen oder regulativen Anforderungen ab. Quellen für Resultate sind dabei:

- Ergebnisse von verschiedenen Protokollen und Scans;
- Statistiken über Schulungen und anderen Aktivitäten;
- Umfrage und Fragebögen;
- Vorfälle;
- Ergebnisse von internen Audits;
- Ergebnisse von Business-Continuity-/Desaster-Recovery-Übungen; und
- Management-Reviews.

Sobald die Quellen bekannt sind, gilt es die Überwachung und Messung, egal ob automatisch oder manuell sowie die Speicherung und Art der Überprüfung festzulegen.

Die Datenüberprüfung kann anhand von Checklisten durchgeführt werden, um sicherzustellen, damit fehlende Daten auf die Analyse nur einen minimalen Einfluss haben und die Werte korrekt sind oder innerhalb anerkannter Grenzen liegen. Zum Zweck der Analyse sollten ausreichend Daten gesammelt werden, um sicherzustellen, dass die Ergebnisse der Analyse zuverlässig sind.

Die Ergebnisse der Analyse werden in der Folge interpretiert. Die durchführende Person sollte in der Lage sein, erste Schlüsse aus den Ergebnissen zu ziehen. Möglicherweise müssen weitere Personen beigezogen werden, die

| Anforderung ISO 27001 | Mögliche Messung |
|---|---|
| 5.1, 7.1 | B.2 Ressourcenzuweisung |
| A.7.2.2 | B.12 Schulung zur Informationssicherheit |

Bild 1: Beispiel.

**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

| | |
|---|---|
| Ziel der Messung | Bewerten, ob die Richtlinien zur Informationssicherheit in geplanten Abständen oder bei wesentlichen Änderungen überprüft werden |
| Auswertung | Prozentsatz der überprüften Richtlinien |
| Berechnung | Anzahl der Richtlinien zur Informationssicherheit, die im Vorjahr überprüft wurden / Anzahl der vorhandenen Richtlinien zur Informationssicherheit * 100 |
| Bewertung | Grün: > 80%, Orange >= 40%, Rot < 40% |
| Nachweis der Analyse | Dokumentenhistorie mit Angabe der Überprüfung des Dokuments oder Dokumentenliste mit Angabe des Datums der letzten Überprüfung |
| Häufigkeit | nach geplantem Intervall, das für Reviews definiert wurde (z.B. jährlich oder nach wesentlichen Änderungen) |
| Verantwortliche Personen | Eigentümer der Richtlinie, der die Verantwortung für die Entwicklung, Überprüfung und Bewertung der Richtlinie übernommen hat<br>Auswertende Person: Interner Auditor<br>Auftraggeber der Messung: CISO |
| Datenquelle | Reviewplan von Richtlinien, Veränderungstabelle einer Sicherheitsrichtlinie, Liste von Dokumenten |
| Format | Kreisdiagramm (Pie Chart) für die aktuelle Situation und Liniendiagramm für die Darstellung der Entwicklung der Compliance |

Bild 2: Überprüfen der Richtlinien

direkt an den technischen und Managementprozessen beteiligt sind, damit die Schlussfolgerungen überprüft und bestätigt werden können.

Die Analyse sollte Lücken zwischen den erwarteten und tatsächlichen Messergebnissen eines implementierten ISMS, Kontrollen oder Gruppen von Kontrollen aufzeigen. Identifizierte Lücken können auf einen Verbesserungsbedarf des implementierten ISMS hinweisen, einschliesslich Richtlinien, Zielen, Kontrollen, Prozessen und Verfahren. Überwachungs-, Mess-, Analyse- und Bewertungsprozesse sollten sich kontinuierlich mit den Anforderungen des ISMS verbessern. Dies beinhaltet:

a) das Feedback der interessierten Parteien;
b) die Überarbeitung der Erfassung- und Analysetechniken auf Grundlage der gemachten Erfahrungen und Rückmeldungen;
c) die Überarbeitung der Umsetzung und Messverfahren; und
d) Resultate zur Informationssicherheit.

Natürlich gilt es die Ergebnisse in einer geeigneten Form aufzubewahren und bei Bedarf zur Verfügung zu haben.

Oft ist es schwierig mit der Messung zu starten. Daher gibt der Anhang B 35 Beispiele von möglichen Messungen. Bild 1 zeigt in der linken Spalte die Anforderungen aus ISO 27001 sowie dem Anhang und verknüpft diese in der rechten Spalte mit einer möglichen Messung. Die Messung-Beispiele enthalten folgende Punkte:

– Ziel der Messung
– Aussage über
– Auswertung
– Berechnung
– Bewertung
– Nachweis der Analyse
– Häufigkeit
– Verantwortliche Personen (Eigentümer, Auswertende Person, Auftraggeber)
– Datenquelle
– Berichtsformat (Bild 2)

Im Bild 3 ist zudem ein Beispiel eines Messberichts zu finden.

| ISO 27001 Anforderung | Messung |
|---|---|
| 5.1, 7.1 | B.2 Resource allocation |
| 7.5.2, A.5.1.2 | B.3 Policy review |
| 5.1, 9.3 | B.4 Management commitment |
| 8.2, 8.3 | B.5 Risk exposure |
| 9.2, A.18.2.1 | B.6 Audit programme |
| 10 | B.7 Improvement actions |
| 10 | B.8 Security incidents cost |
| 10, A.16.1.6 | B.9 Learning form information security incidents |
| 10.1 | B.10 Corrective action implementation |
| A.7.2 | B.11 ISMS training or ISMS awareness |
| A.7.2.2 | B.12 Information security training |
| A.7.2.1, A.7.2.2 | B.13 Information security awareness compliance |
| A.7.2.2 | B.14 ISMS awareness campaigns effectiveness |
| A.7.2.2, A.9.3.1, A.16.1 | B.15 Social engineering preparedness |
| A.9.3.1 | B.16 Password quality – manual |
| A.9.3.1 | B.17 Password quality – automated |
| A.9.2.5 | B.18 Review of user access rights |
| A.11.1.2 | B.19 Physical entry controls system evaluation |
| A.11.1.2 | B.20 Physical entry controls effectiveness |
| A.11.1.4 | B.21 Management of periodic maintenance |
| A.12.1.2 | B.22 Change management |
| A.12.2.1 | B.23 Protection against malicious code |
| A.12.2.1 | B.24 Anti-malware |
| A.12.2.1, A.17.2.1 | B.25 Total availability |
| A.12.2.1, A.13.1.3 | B.26 Firewall rules |
| A.12.4.1 | B.27 Log files review |
| A.12.6.1 | B.28 Device configuration |
| A.12.6.1, A.18.2.3 | B.29 Pentest and vulnerability assessment |
| A.12.6.1 | B.30 Vulnerability landscape |
| A.15.1.2 | B.31.1/B.31.2 Security in third party agreements |
| A.16 | B.32 Security incident management effectiveness |
| A.16.1 | B.33 Security incidents trend |
| A 16.1.3 | B.34 Security event reporting |
| A.18.2.1 | B.35 ISMS review process |
| A.18.2.3 | B.36 Vulnerability coverage |

Bild 3: Ein Beispiel eines Messberichts.

## Fazit

Die ISO 27004 gibt eine genaue Anleitung, wie Messungen definiert und durchgeführt werden sollten und können. Definiert ist, was, wie und wann gemessen und anschliessend ausgewertet wird. Der gesamte Lebenszyklus wird beschrieben. Der Anhang B hilft bei der Suche nach sinnvollen Messungen. Damit stellt die Norm das notwendige Rüstzeug für das Messen und Auswerten von Sicherheitsmetriken dar. Damit nicht nur Mist gemessen wird, sondern das ISMS stetig weiterentwickelt und verbessert wird.