ISO/IEC 27033-1:2023 – Netzwerksicherheit

Die Normenfamilie ISO/IEC 27033 befasst sich mit dem Thema der Sicherheit von Netzwerken. Im Anhang der ISO 27001 hat es einige Massnahmen zur Netzwerksicherheit. Diese werden hier ausführlich behandelt. Sie besteht aus sechs Teilen: Der erste Teil legt die Grundlagen, Begriffe und Konzepte dar und ist damit eine Art Wegweiser durch die restlichen Dokumente. Die weiteren Teile widmen sich dann den konkreten Aspekten: der Planung und Umsetzung von Architekturen (Teil 2), den typischen Szenarien und deren Risiken (Teil 3), Sicherheitsgateways (Teil 4), VPNs (Teil 5) sowie drahtlosen Netzen (Teil 6).

Dieser Beitrag konzentriert sich auf Teil 1, der im September 2023 neu als Schweizer Ausgabe veröffentlicht wurde, inhaltlich aber dem internationalen Text von 2015 entspricht. Er richtet sich nicht nur an Netzwerkadministratoren oder Security-Architekten, sondern explizit auch an Management, Betreiber und Anwender, die mit dem Thema in Berührung kommen.

Scope, Normative Referenzen, Begriffe und Abkürzungen

Das erste Kapitel legt den Anwendungsbereich fest. Netzwerksicherheit wird nicht nur auf die reine Technik beschränkt, sondern umfasst Geräte, deren Verwaltung, die eingesetzten Dienste und Anwendungen sowie die Nutzer. Teil 1 ist als Übersicht gedacht und soll aufzeigen, wie Risiken erkannt, Anforderungen abgeleitet und Kontrollen implementiert werden.

Im zweiten Kapitel werden die normativen Referenzen genannt, darunter die üblichen Eckpfeiler der ISO-27000-Familie: ISO/IEC 27001, 27002, 27005 sowie das OSI-Referenzmodell ISO/IEC 7498.

Das dritte Kapitel listet die wichtigsten Begriffe auf. Dazu gehören Basiskonzepte wie Architektur, Demilitarisierte Zone (DMZ), Intrusion Detection System oder Virtual Private Network. Das Glossar zeigt, dass es nicht nur um technische Geräte geht, sondern um Rollen, Prozesse und Angriffe – von Spoofing bis zur Malware.

Das vierte Kapitel ergänzt zahlreiche Abkürzungen, die im Netzwerkbereich verwendet werden. Von ADSL über IDS, IPS und MPLS bis hin zu VoIP, VLAN und VPN.

Struktur und Überblick

Im fünften Kapitel werden die verschiedenen Teile der ISO 27033 sowie die Struktur des Dokuments erklärt. Das sechste Kapitel bietet eine Übersicht über die Inhalte. Zunächst wird der typische Netzwerkaufbau skizziert, wie er in vielen Firmen vorzufinden ist: Intranet, Erweiterungen als Extranets, der Zugang zum Internet, mobile Nutzer über VPNs oder WLAN, Kommunikation über VoIP. Jede dieser Technologien bringt Chancen, aber auch Risiken, die kurz erwähnt werden. Anschliessend wird der Prozess der Netzwerksicherheitsplanung beschrieben: Risiken erkennen, Anforderungen festlegen, Kontrollen auswählen, Lösungen entwickeln, betreiben und überwachen.

Risiken erkennen und Sicherheitskontrollen planen

Kapitel 7 beschreibt den Einstieg in die Netzwerksicherheitsstrategie: die Sammlung von Informationen. Zuerst wird die eigene Sicherheitsrichtlinie betrachtet. Dort sollten bereits Vorgaben enthalten sein, die unabhängig von einer Risikobewertung gelten, etwa der Einsatz bestimmter Gateways oder die Pflicht zur digitalen Signatur bei Zahlungsaufträgen.

Im nächsten Schritt erfolgt die Analyse der derzeitigen oder der geplanten Netzwerke. Architektur, Anwendungen, Protokolle sowie Dienste sind zu berücksichtigen. Geteilte Netzwerke sind abhörbar, Wireless mit ungenügender Verschlüsselung kann gehackt werden, VPNs sollten sicher konfiguriert werden. Für jede Technologie sind deren Eigenschaften zu betrachten. Selbst die Art der Anwendungen hat Einfluss: Während Messaging-Systeme selbst Verschlüsselung anbieten können, haben Thin-Client-Umgebungen andere Anforderungen.

Die Analyse der Verbindungen ist ebenfalls wichtig: lokal innerhalb des Unternehmens, standortübergreifend, zu Partnern, ins Internet oder ins Telefonnetz. Jedes Verbindungsszenario bringt eigene Risiken mit sich und erfordert andere Massnahmen. Weiter werden Merkmale wie öffentlich oder privat, Daten-, Sprach- oder Hybridnetz erläutert. Zum Abschluss erfolgt eine Kategorisierung, die die Grundlage für die Risikobewertung bildet.

Die Sicherheit in Netzwerken und deren Massnahmen darf nie vernachlässigt werden.

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

Unterstützende Kontrollen

Kapitel 8 fasst die wesentlichen unterstützenden Kontrollen zusammen, die unabhängig von der konkreten Architektur gelten. Dazu gehört das Management der Netzwerksicherheit mit klaren Rollen, Verantwortlichkeiten, Monitoring und Auswertung. Technische Schwachstellen müssen verwaltet, Identitäten verlässlich geprüft, Audit-Logs erstellt und überwacht werden. Intrusion Detection und Prevention werden ebenso erklärt, wie der Schutz vor Schadsoftware und der Nutzung von Verschlüsselungstechniken. Als letztes wird die Wichtigkeit eines Business Continuity Managements aufgezeigt.

Architektur und Referenzszenarien

Kapitel 9 beschreibt die Gestaltung und Umsetzung von Sicherheitsarchitekturen. Am Anfang wird hervorgehoben, dass es keine universelle Lösung gibt. Jedes Unternehmen ist verschieden, hat eine eigene Risikobereitschaft, unterschiedliche Technologien und spezifische Geschäftszielsetzungen. Ein wichtiges Thema ist die Konsistenz. Unkoordiniert eingeführte Kontrollen sind oft der Grund, warum Sicherheitsprobleme entstehen, nicht das Fehlen einzelner Massnahmen. Firewalls, IDS, Verschlüsselung und Authentifizierung – all dies kann seine Wirkung verlieren, wenn es nicht in einer konsistenten Architektur integriert wird. Aus diesem Grund erörtert Kapitel 9, wie Modelle und Frameworks anzuwenden sind.

Kapitel 10 ergänzt dies mit Referenzszenarien, die typische Situationen abbilden: Mitarbeiterzugang ins Internet, Kommunikation zwischen Standorten, B2B- und B2C-Services, Outsourcing, Segmentierung, mobile Kommunikation, Support für Reisende und Homeoffice. Für jedes Szenario werden Risiken und Kontrollen kurz beschrieben.

Das Kapitel 11 ist sehr kurz und listet lediglich 13 Netzwerk-Arten auf, die berücksichtigt werden müssen.

Bild: Pixabay

Umsetzung, Betrieb und Überwachung

Kapitel 12 widmet sich der Entwicklung und dem Test von Sicherheitslösungen. Sobald die technische Sicherheitsarchitektur vollständig dokumentiert und von der Geschäftsleitung genehmigt wurde, sollte die Lösung entwickelt, im «Testmodus» implementiert und gründlich getestet sowie auf ihre Konformität überprüft werden. Sobald die Zweckmässigkeitsprüfung erfolgreich abgeschlossen und alle Änderungen vorgenommen wurden, sollte die Implementierung umgesetzt werden. Vor Abschluss sollten Schwachstellenscans und Penetrationtests durchgeführt werden. Bei solchen Tests sollte beachtet werden, dass ein Netzwerk möglicherweise nicht nur auf ein Land beschränkt ist, sondern sich über verschiedene Länder mit unterschiedlichen Rechtsvorschriften erstrecken kann.

Kapitel 13 ist wiederum sehr kurz und beschreibt den Betrieb: Sicherheitslösungen müssen im Alltag bestehen, gepflegt und angepasst werden.

Das Kapitel 14 betont schliesslich die Notwendigkeit ständiger Überwachung und Überprüfung. Netzwerke ändern sich, Bedrohungen entwickeln sich weiter, und auch die Geschäftsanforderungen sind nie statisch. Nur durch regelmässige Reviews und Anpassungen bleibt die Sicherheit auf dem geforderten Niveau.

Anhang

Anhang A zeigt Querverweise zwischen den Controls aus ISO/IEC 27001 und 27002 (aus dem Jahr 2013, nicht auf die aktuelle Ausgabe) und den Kapiteln dieser Norm. Anhang B liefert ein praktisches Template für Security Operating Procedures (SecOps). Die Norm kann mittels untenstehendem QR-Code gekauft werden.