
Bild: Pixabay

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

ISO/IEC 27033-2 – Netzwerksicherheit planen und umsetzen

Nach dem Überblick in Teil 1 in unserer maschinenbau-Ausgabe 2/26 steigt Teil 2 der Normenreihe ISO/IEC 27033 in die Praxis ein.

Die ISO/IEC 27033 Norm beschreibt, wie aus den definierten Anforderungen eine Sicherheitsarchitektur entsteht, die sowohl die geschäftlichen als auch die technischen Gegebenheiten berücksichtigt und liefert damit eine konkrete Anleitung von der Risikoanalyse zur operativen Umsetzung.

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

Vorbereitung der Netzwerksicherheit

In Kapitel 6 wird hervorgehoben, dass ein gründliches Verständnis der eigenen Umgebung die Grundlage für Netzwerksicherheit ist. Als erster Schritt gilt es, die Werte zu bestimmen, die es zu schützen gilt. Dies umfasst nicht nur physische Geräte wie Router, Firewalls oder Server, sondern auch immaterielle Werte – Konfigurationen, Software, Daten und Geschäftsprozesse. Das Ziel ist es, die Abhängigkeiten zwischen Technologie und Business zu verstehen.

In der Anforderungserhebung, die drei Dimensionen umfasst: rechtliche Vorgaben, geschäftliche Bedürfnisse und Leistungsanforderungen, erfolgt die Anforderungserhebung. Es ist wichtig, rechtliche und regulatorische Anforderungen zu dokumentieren, insbesondere wenn Daten oder Dienste über Ländergrenzen hinweg verlaufen. Geschäftsanforderungen legen fest, wer Zugriff auf was hat, in welchem Umfang und über welche Schnittstellen. Leistungsanforderungen betreffen die Dimensionierung von Leitungen, Gateways und Servern.

Nach dem Sammeln der Informationen erfolgt die Überprüfung der Anforderungen und der bestehenden Netzwerk-Infrastruktur. Es wird untersucht, ob das bestehende oder das in Planung befindliche Netzwerk mit den Sicherheitszielen übereinstimmt. In diesem Schritt wird oft deutlich, dass Anpassungen notwendig sind, wenn bestimmte physische oder technische Gegebenheiten dies erfordern – wie etwa eine einzige verfügbare Leitung, die die Redundanz einschränkt.

Die Vorbereitung endet mit der Beurteilung der aktuellen Sicherheitsmassnahmen. Sie wird mit einer Risikoanalyse gemäss ISO/IEC 27005 verbunden und resultiert in einem Soll-Ist-Vergleich.

Design der Netzwerksicherheit

Das zentrale Element der Norm wird in Kapitel 7 behandelt: die Netzwerksicherheitsarchitektur zu entwerfen. Sie legt fest, wie Datenflüsse zwischen Vertrauensdomänen kontrolliert werden, wo die Übergänge sind und welche Mechanismen an diesen Stellen wirken.

Der Entwurf startet mit einer Analyse der Vertrauensgrenzen – in der Regel zwischen internem Netzwerk und externen Netzwerken, aber auch zwischen verschiedenen internen Zonen. Auf dieser Grundlage werden Sicherheitsdienste festgelegt: Authentifizierung, Zugangssteuerung, Protokollierung, sichere Übertragung, Schwachstellenmanagement, Konfigurationskontrolle, Softwareverteilung und Tests.

Die wichtigsten Designprinzipien sind in Abschnitt 7.2 zusammengefasst:

- Defense in depth: Sicherheit durch Schichten. Alle Ebenen – vom Perimeter über Infrastruktur, Host und Applikation bis zu den Daten – leisten ihren Beitrag. Nach der Norm sind diese Schichten als sich überlappende Verteidigungszonen gedacht, die Redundanz und Fehlertoleranz ermöglichen. Es wird exemplarisch dargestellt, wie Firewalls, Intrusion-Prevention-Systeme und Endpoint-Schutz zusammenwirken.
- Netzwerkzonen: Systeme, die einen unterschiedlichen Schutzbedarf haben, werden in separaten Zonen betrieben. Öffentliche Dienste sollten in eine DMZ platziert werden, während interne Anwendungen in abgeschottete Segmente gehören. Entwicklungs-, Management- und Produktionssysteme sollten ebenfalls strikt vonein-

ander getrennt werden. Technische Mittel wie Sicherheits-Gateways, Firewalls und Access-Lists dienen dazu, diese Zonen abzugrenzen.
- Design Resilience: Es dreht sich nicht nur um Schutzmassnahmen, sondern auch um Widerstandsfähigkeit. Um sicherzustellen, dass ein einzelner Fehler den Betrieb nicht lahmlegt, kommen redundante Schnittstellen, Backup-Module, alternative Wege und Clustertechnologien zum Einsatz.
- Szenarien und Frameworks: Jede Architektur muss in einem Kontext betrachtet werden. Typische Netzwerkszenarien mit spezifischen Risiken sind in ISO/IEC 27033-3 zu finden, während die Teile 4 bis 6 sich mit einzelnen Technologien (Gateways, VPNs, Wireless) befassen. Teil 2 nennt auch das ITU-T-Framework X.805, das Sicherheitsdimensionen und -schichten definiert und sich mit den Massnahmen aus der ISO/IEC 27001 verbinden lässt.

In Abschnitt 7.3 wird zudem eine formale Design-Freigabe durch das Management gefordert.

Umsetzung der Netzwerksicherheit

Die praktische Umsetzung wird in Kapitel 8 behandelt. Das genehmigte Design ist dabei der Ausgangspunkt. Die Umsetzung beinhaltet die Segmentierung, Auswahl der Komponenten und Produkte, Management, Monitoring, Dokumentation und Tests.

Komponentenauswahl: Die Norm listet eine Vielzahl von Bausteinen auf: Firewalls, Router, VPN-Gateways, IDS/IPS, Endpoint-Schutz, Verschlüsselung, Authentifizierungssysteme, Content-Filter, Netzwerkzugangskontrollen und Management-Systeme. Entscheidend dabei ist, wie sie kombiniert werden. Nicht jedes Element ist überall nötig, aber sie müssen zusammen das festgelegte Schutzniveau erreichen.

Auswahl von Produkten und Lieferanten: Die Bewertung von Produkten sollte anhand technischer und organisatorischer Kriterien erfolgen. Dazu gehören Kompatibilität, Leistung, unterstützte Protokolle, Skalierbarkeit, Dokumentation, Wartbarkeit, Sicherheitszertifizierung (zum Beispiel nach ISO 15408) und die Verlässlichkeit des Herstellers. Der Fokus liegt darauf, Vertrauen in die Lieferkette aufzubauen und Abhängigkeiten bewusst zu steuern.

Netzwerkmanagement: Die sichere Verwaltung steht bei diesem Punkt im Fokus. Unterschieden werden von der Norm organisatorische und technische Kontrollen. Organisatorisch sind klare Rollen, das Vier-Augen-Prinzip und Berechtigungsprozesse von Bedeutung. Auf technischer Ebene sind sichere Administrationsschnittstellen, Protokolle mit Verschlüsselung und starker Authentifizierung erforderlich, zum Beispiel mit SSH oder VPN geschützt. Die Norm weist unter anderem darauf, nur noch SNMP v3 zu nutzen, da die vorherigen Versionen als unsicher gelten.

Protokollierung, Überwachung und Incident Response: Alle sicherheitsrelevanten Vorfälle sollten zentral erfasst werden. In einer geschützten Zone aggregiert ein Audit-Server die Logs von Firewalls, Servern und weiteren Komponenten. Zugriff haben ausschliesslich autorisierte Sicherheitsverantwortliche. Automatische Benachrichtigungen (E-Mail, SMS) müssen Anomalien umgehend melden.

Dokumentation: Ein umfassendes Architektur- und Sicherheitsdokument ist Pflicht. Es umfasst Anforderungen, technische Spezifikationen, Firewall-Regeln, Analyseberichte sowie Testergebnisse. Entsprechende Templates sind im Anhang B zu finden.

Prüfungen: Bevor das Gerät in Betrieb genommen wird, sind Sicherheitsprüfungen geplant und umgesetzt. Dies umfasst Authentifizierungs- und Autorisierungstests sowie Überprüfungen der Härtung, des Loggings und der Resilienz. Es ist wichtig, dass Testdaten und -szenarien klar und nachvollziehbar dokumentiert werden. Nach der erfolgreichen Testphase erfolgt wiederum der Abschluss durch ein formales Sign-off des Managements.

Anhänge

Der Anhang A stellt die Verbindung zwischen den beiden Normen ISO 27001 und ISO 27033-2 her. Im Anhang B sind wie zwei Templates (besser Inhaltsverzeichnis) vorhanden: Netzwerk-Sicherheitsarchitektur sowie funktionale Sicherheitsanforderungen.

Der Anhang C zeigt, wie das ITU-T-Framework X.805 als Ergänzung zur ISO/IEC 27001 genutzt werden kann. Über drei Ebenen (Infrastruktur, Services, Anwendungen) und drei Steuerungsebenen (Management, Control, User Plane) betrachtet das Modell Netzwerke und weist ihnen acht Sicherheitsdimensionen zu. Unter anderem Zugriffskontrolle, Integrität, Verfügbarkeit oder Vertraulichkeit.

Fazit

Die ISO/IEC 27033-2 ist der praxisorientierte Teil der Reihe. Sie erklärt nicht nur, was die Netzwerksicherheit erreichen soll, sondern auch, wie ein Unternehmen Schritt für Schritt dorthin gelangt. Die Norm zeigt eine klare Methodik, die technische, organisatorische und regulatorische Aspekte verbindet, von der Erfassung der Assets über Designprinzipien wie Defense in Depth bis hin zur Dokumentation und Testphase.

REGO-FIX

toolVibe®

Sensorischer
Werkzeughalter –
schnell und einfach

www.rego-fix.com