ISO/IEC 27033-3 – Netzwerksicherheit in der Praxis

Mit dem dritten Teil der Reihe wird die ISO/IEC 27033 konkret. Während Teil 1 die Konzepte definiert und Teil 2 das Vorgehen für Design und Implementierung beschreibt, liefert Teil 3 praxisnahe Referenzszenarien. Sie zeigen, wie sich Netzwerksicherheit in unterschiedlichen Geschäftssituationen umsetzen lässt.

Das Ziel dabei ist nicht, einzelne Produkte oder Technologien vorzugeben, sondern das Denken in Szenarien zu fördern. Jede Umgebung hat eigene Risiken und braucht darauf abgestimmte Kontrollen.

Überblick

Die Norm folgt einem einheitlichen Aufbau: Zuerst wird der Kontext dargestellt, dann die typischen Bedrohungen und schliesslich die passenden Designprinzipien sowie Sicherheitskontrollen. Die Grundlage bildet die Risikoanalyse aus Teil 2, ergänzt durch die Bedrohungstaxonomie, die in Anhang B zu finden ist.

Teil 3 umfasst neben den klassischen Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit auch weitere Aspekte wie Authentizität, Nachvollziehbarkeit (Non-Repudiation) und Opazität (Englisch: Opacity). Letztere bezieht sich auf den Schutz von Handlungen, wie beispielsweise das Verbergen, dass eine Kommunikation überhaupt stattgefunden hat.

Internetzugang für Mitarbeitende

Im ersten Szenario steht der kontrollierte Internetzugang im Fokus. Es ist wichtig, dass Unternehmen bestimmen, wofür der Internetzugang genutzt werden darf: ausschliesslich geschäftlich oder auch privat, und in welchem Umfang.

Die wesentlichen Risiken sind Malware, Datenabfluss, unautorisierte Nutzung und Haftungsfragen. Die Norm empfiehlt: nur geschäftsrelevante Dienste freischalten, Antiviren-Scanner an Gateway und auf Clients, Inhaltsfilter und Whitelists, klare Nutzungsrichtlinien und Schulung der Mitarbeitenden. Ein Beispiel für eine Internetnutzungsrichtlinie ist im Anhang A abgebildet.

Business-to-Business-Verbindungen

In Kapitel 8 der Norm stehen die Beziehungen zwischen Organisationen, das heisst Lieferanten, Partnern, Dienstleistern, im Fokus. Die wichtigsten Schutzziele sind die Verfügbarkeit und die Integrität. Typische Bedrohungen umfassen Malware, DoS-Angriffe, Insider-Missbrauch oder gefälschte Transaktionen.

Die empfohlenen Massnahmen umfassen Antivirus-Kontrollen an den Übergängen, festgelegte Rollen und Verantwortlichkeiten, Protokollierung aller Vorgänge, digitale Signaturen für Transaktionen und klar geregelte Zugriffsbeschränkungen.

Business-to-Customer-Dienste

Im dritten Szenario wird das Spannungsfeld zwischen Benutzerfreundlichkeit und Schutzbedarf dargestellt. Dies betrifft unter anderem E-Commerce, Online-Banking oder E-Government.

Die Angriffe variieren von Phishing und SQL-Injection über Session Hijacking bis hin zu «Man-in-the-Browser»-Attacken. Die Strategie zur Abwehr dieser Bedrohungen: Netzwerk in Zonen aufteilen, DMZ einrichten, strenge Authentifizierung, Verschlüsselung mit SSL/TLS, rollenbasierte Zugriffskontrolle, Intrusion Detection und Protokollierung. Die sichere Architektur muss die Informationssicherheit gewährleisten, nicht punktuelle Filter.

Kollaborationsdienste

Gemeinsames Arbeiten ist Alltag – sei es durch Datei-Sharing, E-Mail, webbasierte Dienste oder Videokonferenzen. Dieses Kapitel beschreibt, wie solche Systeme intern und extern sicher betrieben werden können.

Mögliche Gefahren sind: unbefugter Zugriff, Malware über gemeinsame Ressourcen und Überlastung durch legitimen Verkehr. Zu den Gegenmassnahmen zählen Zugriffsrechte basierend auf Rollen, VLAN-Trennung, Verschlüsselung, IDS auf Hostebene, Einschränkung von Dateiübertragungen und Überwachung der Nutzung.

Netzwerksegmentierung

Die Segmentierung als strukturelles Sicherheitsmittel wird in Kapitel 11 der Norm behandelt. Netzwerke sollten getrennt werden, basierend auf organisatorischen

Die Sicherheit in Netzwerken und deren Massnahmen darf

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

und rechtlichen Anforderungen, zum Beispiel nach Ländern, Geschäftsbereichen oder Sensitivitätsstufen. Die Norm listet unter anderem die Trennung von administrativen Aufgaben gegenüber normalen Benutzerzugriffen, die Trennung von kritischen Anwendungen sowie Datenbanken von Benutzern und Systemen.

Das schützt nicht nur technische Systeme, sondern erleichtert auch die Einhaltung gesetzlicher Vorgaben, etwa die Datenschutz-Anforderungen. Die Norm empfiehlt die Nutzung von Security Gateways, Applikationsproxies, Verschlüsselung und verbindliche Awareness-Programme.

Homeoffice und kleine Büros

Heimarbeitsplätze oder kleine Standorte ins Unternehmensnetz zu integrieren, bringt eigene Herausforderungen mit sich. Private Geräte werden gemeinsam genutzt, und die vorhandene Infrastruktur ist oft minimal.

Risiken wie schwache Routerkonfigurationen, fehlende Updates, Viren, Datenlecks durch nicht gesperrte Geräte oder herumliegende Dokumente, aber auch falsche WLAN-Einstellungen können gefährlich sein.

Bild: Pixabay

nie vernachlässigt werden.

Die Norm empfiehlt: Firewalls einschalten, ungenutzte Schnittstellen abschalten, starke Passwörter erzwingen, VPN-Verbindungen nutzen, regelmässige Updates durchführen und Nutzende sensibilisieren.

Mobile Kommunikation

Mobile Geräte sind eine besondere Herausforderung für jedes Unternehmen. Geräte werden oft privat beschafft und sowohl für private Dinge wie auch geschäftliche Aufgaben genutzt. Zudem sind sie immer online.

Die Hauptrisiken sind: Verlust oder Diebstahl, fehlende Zugriffskontrolle, Malware, unverschlüsselte Datenübertragung oder unbeabsichtigte Standortfreigabe. Die Norm nennt als Gegenmassnahmen: Verschlüsselung von gespeicherten und übermittelten Daten, starke Authentifizierung, automatische Sperren, Nutzung eines Mobile-Device-Managements, Remote-Wipe-Funktion (Fern-Löschung), regelmässige Updates und klare Nutzungsrichtlinien.

Die Norm hat auch ein Kapitel für «reisende Mitarbeitende». Dies tönt etwas veraltet. Heute können die Gefahren und Massnahmen der mobilen Kommunikation berücksichtigt werden.

Ausgelagerte Dienste

Das letzte Szenario behandelt das Thema Outsourcing – sei es für Support oder Entwicklung. In diesem Fall verlagert sich die Verantwortung teilweise auf externe Partner, was Abhängigkeiten und neue Risiken zur Folge hat.

Die Norm listet eine Vielzahl von Gefährdungen auf, darunter unbefugter Zugriff auf andere interne Systeme (zum Beispiel durch Support), Missbrauch von Administratorrechten, mangelnde Rücksicht auf die Rechte an geistigem Eigentum, mangelnde Best Practices für die Informationssicherheit oder ungenügende Haftung bei Verstössen gegen Vorschriften.

Die Norm verlangt: strikte Zugriffskontrolle mit persönlichen Logins, Zwei-Faktor-Authentifizierung, umfassendes Logging, Verschlüsselung sensibler Informationen, vertraglich festgelegte Minimal-Anforderungen, Auditrechte, Schulungen der eingesetzten Mitarbeitenden und die Einhaltung der lokalen Datenschutzgesetze.

Anhänge

Wie bereits erwähnt ist im Anhang A eine ausführliche Internet-Nutzungsrichtlinie vorhanden. Der Anhang B listet zu 17 Themen diverse Gefährdungen auf.