7 Sicherheitskonzept

Einleitung

Durch Sicherheitsmaßnahmen sollen Störungen und dadurch auch Schäden vermieden werden. Dabei sind die Randbedingungen äußerst herausfordernd: vielfältige technische Systeme müssen berücksichtigt werden, die fachlichen und betrieblichen Abläufe sind komplex, die Dynamik der technischen Weiterentwicklung hoch und die Ressourcen im Security-Team gewöhnlich knapp. Angesichts einer solchen Ausgangssituation ist es offensichtlich, dass Einzelmaßnahmen nur zu einem Sicherheitsflickenteppich führen würden – Sicherheitslücken blieben zwangsläufig bestehen.

Chancen auf ein durchgängiges Sicherheitsniveau bestehen nur, wenn die Organisation durch ein Informationssicherheits-Managementsystem (ISMS) eine systematische Vorgehensweise etabliert. Beim ISMS liegen die Steuerungsaufgaben: Definition der Unternehmensleitlinie, Aufbau der Informationssicherheitsorganisation, Bereitstellen von Ressourcen, Treffen der erforderlichen Entscheidungen zur Umsetzung auf Management-Ebene sowie Management-Reviews und Vorgaben zur Verbesserung der Informationssicherheitsorganisation.

Die Verantwortlichen in der Informationssicherheitsorganisation müssen Maßnahmen festlegen, mit denen auf Sicherheitsprobleme angemessen reagiert wird. Nur wenn nachvollziehbar dokumentiert ist, wie Sicherheitsmaßnahmen aufeinander abgestimmt sind und welche Lücken verbleiben, kann beurteilt werden, ob das gewünschte Sicherheitsniveau erreicht wird und die angestrebten oder umgesetzten Maßnahmen angemessen sind. Das Sicherheitskonzept kann dies auf einem hohen Abstraktionsniveau darstellen: Hier werden die Strategien und Entscheidungen festgelegt, mit denen auf relevante Risiken, Gefährdungen, Angreifermodelle und Schwachstellen reagiert werden soll (siehe auch Abschnitt 1.1.5). Wegen seiner zentralen Bedeutung sollen daher in diesem Abschnitt die Kernelemente des Sicherheitskonzepts dargestellt werden. Die Reihenfolge der weiteren Kapitel dieses Buchs wurde an der Abfolge dieser Darstellung orientiert.

7.1 Ziele des Sicherheitskonzepts

Ziel eines Sicherheitskonzepts ist es, auf einem hohen Abstraktionsniveau die baulichen, technischen, organisatorischen und personellen Maßnahmen der Informationssicherheit darzustellen. Mit dem Sicherheitskonzept soll gezeigt werden, dass und wie die Sicherheitsprobleme auf dem für die Organisation angestrebten Sicherheitsniveau beherrscht werden. Durch eine systematische Vorgehensweise und die vollständige Abdeckung sollen nicht akzeptable Schwachstellen vermieden werden.

Ausgangspunkt des Sicherheitskonzepts sind die Ergebnisse einer vorgelagerten Risikoanalyse. Für die relevanten Risiken werden im Sicherheitskonzept Maßnahmen definiert, die in ihrem Zusammenwirken diese Risiken auf das von der Organisation akzeptierte Maß reduzieren. Abstrakt bedeutet in diesem Zusammenhang, dass bei der Definition

der Maßnahmen weitgehend auf Details der Umsetzung verzichtet wird. Diese Aspekte werden erst in nachgelagerten Dokumenten beschrieben.

Das Sicherheitskonzept enthält daher vor allem eine abstrakte Sicherheitsarchitektur und abstrakte Sicherheitsmaßnahmen. Außerdem sollte abstrakt die Stärke der Mechanismen, die die Maßnahmen erreichen sollen, und die Kriterien, wann diese Vorgaben gelten, festgelegt werden. So könnte beispielsweise gefordert werden, dass Datenbestände mit einer bestimmten Vertraulichkeitseinstufung nur mit zwei-Faktor-Authentifzierung oder im vier-Augen-Prinzip eingesehen werden dürfen. Die Maßnahmen müssen mit den Anforderungen der Geschäftsprozesse und den Betriebskonzepten für Techniksysteme abgestimmt sein. So müssen möglicherweise für die zu einem Dienstleister ausgelagerten Systeme andere Maßnahmen ergriffen werden, als für die Systeme, die im eigenen Rechenzentrum betrieben werden.

Abschließend sollte das Sicherheitskonzept die Bewertung des konzipierten Sicherheitsniveaus und die verbleibenden Risken zusammenfassend darstellen.

Damit bietet das Sicherheitskonzept die Möglichkeit, die Auswahl der abstrakten Sicherheitsmaßnahmen und ihr Zusammenwirken zu überprüfen. Die getroffenen Entwurfsentscheidungen bilden die Grundlage der Umsetzung von Sicherheitsmaßnahmen z. B. durch die konkrete Gestaltung betrieblicher Prozesse oder für die Auswahl und Gestaltung technischer Systeme. Das Konzept leistet darüber hinaus Argumentationshilfe bei unternehmenspolitischen Entscheidungen zur Durchsetzung von Maßnahmen. Dies ist insbesondere wichtig, wenn angesichts knapper Ressourcen Prioritäten gesetzt werden müssen.

Aus dem Sicherheitskonzept ergeben sich Aufgaben, durch die die Maßnahmen umgesetzt, betreut und fortgeschrieben werden. Seine Wirkung kann das Konzept nur entfalten, wenn für diese Aufgaben die Zuständigkeiten geklärt, Prozesse etabliert und Ressourcen bereitgestellt werden. Die Aufbau- und Ablauforganisation für Informationssicherheit müssen mit den Entscheidungen im Sicherheitskonzept harmonieren. Es kann sinnvoll sein, die Rollen, die die Umsetzung steuern, sowie wichtige Prozesse, mit deren Hilfe Maßnahmen realisiert werden, im Sicherheitskonzept zu benennen. Das Sicherheitskonzept bietet dann auch eine Checkliste, um den Stand der Umsetzung zu prüfen.

Auch für die Vorbereitung von Sicherheitsaudits bietet das Sicherheitskonzept wertvolle Informationen. Es gibt einen Überblick über die ergriffenen Maßnahmen. Daraus und aus einer Änderungshistorie des Sicherheitskonzepts können Audit-Schwerpunkte abgeleitet werden. Dazu könnten im Sicherheitskonzept auch Kennzahlen festgelegt werden, über die im Management-Report zu berichten ist. Das Sicherheitskonzept ist damit ein zentrales Ergebnis der Abstimmungsprozesse innerhalb der Sicherheitsorganisation und zum zum Managementsystem für Informationssicherheit. Einen Überblick über die Aufgaben, die im Rahmen eines Informationssicherheits-Managementsystems abzudecken sind, geben Standards, z. B. *ISO 27001* (Kapitel 5) oder das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Konzept des IT-Grundschutzes (Kapitel 6) samt der vielfältigen Umsetzungsmaterialien.

Einordnung in die Dokumentationsstruktur

Das Sicherheitskonzept ist ein Dokument der Planungsebene. Es beschreibt primär das Gesamtbild für die Lösung der Aufgabe »Informationssicherheit«. Für dieses Ziel sollte die Beschreibung auf einer einheitlichen Abstraktionsebene erfolgen. Gegebenenfalls

wird das übergreifende Sicherheitskonzept durch nachgeordnete Konzepte für einzelne Sicherheitsbereiche detailliert, beispielsweise zur Netzwerksegmentierung, zu Firewalls oder dem Business-Continuity-Management.

Sowohl die Abgrenzung als auch die Bezüge des Sicherheitskonzepts zur übrigen Sicherheitsdokumentation, z. B. der Risikoanalyse, der Sicherheitsleitlinie oder den Umsetzungsdokumenten sollten klargestellt werden.

Fortschreibung

Damit das Sicherheitskonzept ein aktuelles Gesamtbild der Maßnahmen zur Informationssicherheit gibt, muss es – wie andere Dokumente der Informationssicherheit auch – in die Aktualisierungsprozesse einbezogen werden. Auslöser für Aktualisierunsbedarf können beispielsweise sein: veränderte Management-Vorgaben zur Informationssicherheit, veränderte Risikobewertungen, auf die bereits durch Konzept-Änderungen reagiert werden soll, Änderungen in der Maßnahmenstrategie, wenn z. B. ein bisheriges einheitliches Netzwerk in VLANs aufgeteilt werden soll oder Aktualisierungen von Standards.

7.2 Zentrale Aufgaben im Sicherheitskonzept

Das Ziel von Sicherheitsmaßnahmen ist es, Störungen zu vermeiden und im Störfall schnell und wirkungsvoll reagieren zu können. Ein Sicherheitskonzept muss daher mindestens für die folgenden zentralen Aufgaben abstrakt beschreiben, welchen Stellenwert sie haben und mit welcher Vorgehensweise und welchen Maßnahmen sie gelöst werden:

- die Abgrenzung Berechtigter und Unberechtigter voneinander,
- das Vermeiden von Schwachstellen,
- das Erkennen von Unregelmäßigkeiten und
- die Reaktionen auf Störungen.

Die Seminareinheiten, die sich in der T.I.S.P.-Schulung mit Sicherheitsmaßnahmen befassen, werden in den folgenden Abschnitten unter diese zentralen Aufgaben gruppiert. Diese Zuordnung richtet sich nach dem vorrangigen Nutzen einer Maßnahme. Viele der Maßnahmen haben allerdings Wirkungen für mehr als eine der zentralen Aufgaben. Dies können Sicherheitsgewinne sein; teilweise stehen Maßnahmen, die eine Aufgabe unterstützen aber auch im Konflikt zu anderen Aufgaben im Sicherheitskonzept.[1] Dies muss bei der Entwicklung des Konzepts geeignet berücksichtigt werden.

7.2.1 Berechtigte und Unberechtigte

Eine sehr wichtige Aufgabe für die Sicherung einer IT-Landschaft im Betrieb ist es, Unberechtigte daran zu hindern, IT-Systeme und die durch sie bereitgestellten Funktionen zu nutzen und Datenbestände einsehen oder gar ändern zu können. Dies gelingt nur, wenn sowohl physischer Zutritt als auch der Zugriff auf Systeme, Daten und Anwendungen so

1 Siehe dazu z. B. die Zielkonflikte zwischen Verschlüsselung und Datensicherung, die in Kapitel 25 dargestellt sind

kontrolliert werden können, dass nur Berechtigte die Ressourcen nutzen können. Durch Maßnahmen der *physischen Sicherheit* (Kapitel 8) wird verhindert, dass Unbefugte Zutritt zu den IT-Systemen und Datenträgern erhalten. Informationssysteme werden heute fast immer innerhalb eines Netzwerks betrieben. Grundlagen der *Netzwerksicherheit* (Kapitel 9) helfen daher, sicherheitsrelevante Entscheidungen für den Aufbau des Netzwerks zu treffen. Mithilfe von *Firewalls* (Kapitel 10) wird eine angemessene Abgrenzung zwischen den Weiten des Internets und den geschützten Bereichen des internen Netzwerks einer Organisation geschaffen. Firewalls stellen deshalb einen wesentlichen Baustein der Zugangs- und Zugriffskontrolle dar.

Auch mithilfe *kryptografischer Verfahren* (Kapitel 11) soll eine Abgrenzung zwischen Berechtigten und Unberechtigten erreicht werden. Ihr Einsatz gilt häufig dem Schutz vertraulicher Informationen vor unberechtigter Kenntnisnahme. Kryptografische Verfahren sind aber auch für vielfältige weitere Sicherheitsmaßnahmen nutzbar. Zu ihrem umfassenden Einsatz im Unternehmen ist in der Regel der Aufbau von *Public Key Infrastrukturen* (PKI) erforderlich. Sie werden in einem eigenen Kapitel mitsamt den zugehörigen *Vertrauensmodellen* und Standards beschrieben (Kapitel 12).

Kryptografische Verfahren finden auch Verwendung bei der Absicherung von Netzwerkverbindungen, z. B. für den Aufbau von *Virtual Private Networks* (VPN, Kapitel 13) und zur Absicherung von *mobilen Netzen* (Kapitel 14).

Nicht alle Berechtigten dürfen in der Regel gleichermaßen alle Funktionen und Daten verwenden. Die Gestaltung von *Authentifizierung und Berechtigungsmanagement* (Kapitel 15) und die Differenzierung der Zugriffsberechtigungen sind daher weitere zentrale Bausteine der Zugriffskontrolle. Neben den Authentifizierungsmechanismen der Benutzeranmeldung können auch weitere der vorgenannten Maßnahmen einen wichtigen Beitrag zur Authentifizierung und damit der Abgrenzung zwischen Berechtigten und Unberechtigten leisten, z. B. kryptografische Verfahren im VPN. Weitere zentrale Mechanismen des Berechtigungsmanagements werden im Zusammenhang mit Betriebssystemen dargestellt.

7.2.2 Schwachstellen vermeiden

Selbst wenn es Unberechtigten gelingen sollte, die realisierten Vorkehrungen zu ihrer Abwehr zu überwinden, sollen sie möglichst wenige Ansatzpunkte haben, um Schaden anzurichten. Es ist daher wesentlich, innerhalb der Systeme möglichst alle Schwachstellen zu vermeiden. Dies gilt ganz besonders auf Ebene der Betriebssysteme. Aus diesem Grund stellt zunächst das Kapitel *Betriebssystemsicherheit* unabhängig von konkreten Implementierungen die Sicherheitsaufgaben und -probleme von Betriebssystemen vor (Kapitel 16). Diese Aspekte werden dann in je einem Kapitel für die Betriebssysteme *Windows* (Kapitel 17) und *Unix* (Kapitel 18) vertieft. Der immer größeren Bedeutung *mobiler Endgeräte* trägt Kapitel 19 mit einem Blick auf deren Sicherheitsmechanismen Rechnung.

Immer mehr Anwendungen sind auch aus dem Internet zugänglich. Dort führen Schwachstellen zu besonders hohen Risiken. Kapitel 20 widmet sich daher der Sicherheit von Anwendungssystemen unter besonderer Berücksichtigung von Web-Interfaces.

Da nicht vorhandene Daten nicht missbraucht werden können, trägt das sichere *Löschen und Entsorgen* (Kapitel 21) nicht mehr benötigter Daten oder Datenträger ebenfalls zur Vermeidung von Schwachstellen bei. Es dient der Sicherung der Vertraulichkeit und

trägt den Datenschutzprinzipien Zweckbindung, Datenminimierung und Speicherbegrenzung nach DSGVO Rechnung.

Die bisher aufgeführten Maßnahmen sind im Wesentlichen technisch ausgerichtet. Es darf aber nicht vergessen werden, dass Menschen die erdachten Vorgaben umsetzen und einhalten müssen. Auf deren Kooperation kann nur zählen, wer die – häufig wenig intuitiven und oft behindernden – Sicherheitsvorgaben erläutert und Verständnis für die Notwendigkeit weckt. Dies muss durch Information, Schulung und die Schärfung des Problembewusstseins in Awareness-Maßnahmen (Kapitel 22) erreicht werden.

7.2.3 Identifikation von Unregelmäßigkeiten

Hat man die Möglichkeiten für Angriffe und unbeabsichtigte Störungen reduziert, besteht die nächste Aufgabe darin, dennoch auftretende Unregelmäßigkeiten zu erkennen. Unter Unregelmäßigkeiten werden hier Abweichungen vom Regelverhalten oder von Regelprozessen verstanden, die eine relevante Schwelle überschreiten. Außer über das herkömmliche System-Monitoring können Unregelmäßigkeiten beispielsweise mit Sicherheitsanwendungen identifiziert werden, die Angriffe über Kommunikationsinhalte erkennen (*Content Security*, Kapitel 23) und Angriffe durch Computer-Viren oder andere Malware abwehren sollen. *Intrusion-Detection-Systeme* (IDS, Kapitel 24) zielen dagegen stärker auf die Überwachung des Nutzerverhaltens, um unzulässige Aktionen Unberechtigter und gegebenenfalls auch berechtigter Nutzer zu identifizieren. Ein solches System kann zum Beispiel ungewöhnliche Muster beim Zugriff auf Dateien, Programme und Netzsegmente erkennen und eine automatische Warnung auslösen.

Erkannte Unregelmäßigkeiten müssen analysiert und bewertet werden. Daraus kann sich ergeben, dass ein Störfall vorliegt, für den ein Eingreifen erforderlich ist.

7.2.4 Reaktionen auf Störfälle

Trotz aller Vorsorge durch die in den vorangegangenen Abschnitten genannten Sicherheitsmaßnahmen können Störfälle auftreten. Dann sind Reaktionen erforderlich – die Organisation soll auch in solchen Situationen handlungsfähig sein. Eine wichtige Voraussetzung für viele Reaktionen auf Sicherheitsvorfälle ist die Möglichkeit, alte System- oder Informationsstände wieder herzustellen. Mit dem Thema *Datensicherung* beschäftigt sich deshalb das Kapitel 25.

Durch *Computer Emergency Response Teams* soll effizient auf Angriffe reagiert werden. Deren Aufgaben und der Incident-Prozess werden in Kapitel 26 vorgestellt. Damit nicht nur auf kleinere Störfälle, sondern auch auf weitreichende Krisen reagiert werden kann, sollten Organisationen schließlich auch ein *Business-Continuity-Management* (Kapitel 27) aufbauen.

Zusammenfassung

Die Entwicklung eines Sicherheitskonzepts ist eine zentrale Aufgabe der Informationssicherheitsorganisation. Dieses Konzept stellt die Sicherheitsarchitektur und das Zusammenwirken der abstrakten Sicherheitsmaßnahmen dar und ist Teil der Sicherheitsdokumentation. Es stellt Risiken und abwehrende Maßnahmen gegenüber und ermöglicht so, das Sicherheitsniveau auf einer abstrakten Ebene zu prüfen. Zentrale Aufgaben des Sicherheitskonzepts sind, Maßnahmen zur Abgrenzung zwischen Berechtigten und Unberechtigen, zur Vermeidung von Schwachstellen, zur Identifikation von Unregelmäßigkeiten und zur Reaktion auf Störfälle zu definieren. Das Konzept umfasst für die genannten Aufgaben alle abstrakten baulichen, organisatorischen, technischen und personellen Maßnahmen, die zum Erreichen der Sicherheitsziele der Organisation beitragen.

Ein vollständiges und systematisch aufgebautes Sicherheitskonzept ist das Steuerungsinstrument, mit dem ein einheitliches und angemessenes Sicherheitsniveau festgelegt werden kann.

Literatur

[FoxJen09] *Fox, D.; Jendrian, K.:* Struktur von Sicherheitsleitlinien, DuD 5/2009, 313 ff. *http://www.secorvo.de/publikationen/sicherheitsrichtlinien-fox-jendrian-2009.pdf*