



SAVE Security Services

Etablieren von unternehmensweiten IT-Sicherheitsprozessen

White Paper

Erstellung von IT-Sicherheitskonzepten

Überblick

Ein IT-Sicherheitskonzept stellt einen Plan zur Erhaltung oder Verbesserung der IT-Sicherheit in einer Organisation dar. Es beschreibt, welche IT-Sicherheitsanforderungen das Unternehmen hat und welche Maßnahmen zur Umsetzung dieser Anforderungen bereits ergriffen wurden bzw. ergriffen werden sollen. Dabei sind die folgenden Fragen zu beantworten: Welche Werte müssen geschützt werden? Wovor müssen sie geschützt werden? Welche Aufwände für Analysen und Gegenmaßnahmen sind den identifizierten Schwachstellen und Bedrohungen angemessen? Welche Sicherheitsmaßnahmen sollen ergriffen werden? Das IT-Sicherheitskonzept ist somit das zentrale Dokument im IT-Sicherheitsprozess eines Unternehmens bzw. einer Behörde. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen.

Für die Erstellung eines IT-Sicherheitskonzepts ist ein systematisches Vorgehen unerlässlich, da nur so sichergestellt werden kann, dass alle relevanten Aspekte betrachtet werden und keine vermeidbaren Lücken in der IT-Sicherheit verbleiben. Als Stand der Technik hat sich eine Methodik etabliert, die auf den folgenden Schritten beruht:

- *IT-Strukturanalyse* – Festlegung des Umfangs und Aufbaus der zu schützenden IT;
- *Schutzbedarfsfeststellung* – Bestimmung des erforderlichen Sicherheitsniveaus;
- *Modellierung* – Identifikation von Standardkomponenten in der IT und ihrem Umfeld;
- *Schwachstellenanalyse* – Identifikation möglicher Angriffe und Sicherheitslücken;
- *Maßnahmenplanung* – Festlegung der notwendigen Schutzmaßnahmen;
- *Risikokontrolle* – Identifikation und ggf. Akzeptanz der trotz Maßnahmen verbleibenden Risiken.

Diese Schritte werden hier kurz erläutert.

Methodik

Die **IT-Strukturanalyse** dient der Vorerhebung von Informationen, die für die weitere Vorgehensweise in der Erstellung eines IT-Sicherheitskonzepts benötigt werden. Sie gliedert sich in folgende Teilaufgaben:

- *Netzplanerhebung* – Festlegung und Abgrenzung des Untersuchungsbereichs und der Objekte
- Erfassung der IT-Anwendungen und der zugehörigen Informationen
- Erhebung der IT-Systeme, Räume und Kommunikationsverbindungen
- Komplexitätsreduktion durch *Gruppenbildung* – Modularisieren gleichartiger Systeme

Eine Bedrohung der Sicherheit des IT-Systems und seiner Anwendung(en) ist dann gegeben, wenn wesentliche Leistungsziele, die mit dem Einsatz des IT-Systems bezweckt werden, beeinträchtigt werden oder beeinträchtigt werden können. Die Erwartungen, die hinsichtlich der Schutzfunktionen an ein IT-System gestellt werden, die *Sicherheitsanforderungen*, lassen sich mit Hilfe von gewissen Globalanforderungen formulieren. Im Sinne einer dualen Sicherheit wird vom IT-System

- der Schutz der *Vertraulichkeit* der Daten und Vorgänge im IT-System;
- der Schutz vor unzulässigen Veränderungen der im IT-System gespeicherten Daten und der Verarbeitungsprozesse (*Integrität*);
- die kontinuierliche *Verfügbarkeit* seiner Leistungen und der dort gespeicherten Daten und
- die Möglichkeit des revisionsfähigen Nachweises der Urheberschaft der Daten im Sinne von Authentizität und Nicht-Abstreitbarkeit (Verbindlichkeit).

verlangt.

Anforderungen

Eine IT-Sicherheitsanalyse und die Erstellung eines IT-Sicherheitskonzepts erfolgt oft nicht ausschließlich im Rahmen eines Informationssicherheits-Managements. Beispiele hierfür sind: Die Planung einer geeigneten Notfallvorsorge ist abhängig von klar identifizierten Verfügbarkeitsanforderungen. Die datenschutzrechtlichen Forderungen verlangen die Implementierung wirksamer technisch-organisatorischer Schutzmaßnahmen, die – abhängig vom bereichsspezifischen Datenschutzgesetz – sogar explizit in Form eines IT-Sicherheitskonzepts vorzulegen sind.

Die genauen Sicherheitsanforderungen werden bei Erstellung eines IT-Sicherheitskonzepts im Rahmen der **Schutzbedarfsfeststellung** ermittelt, um die konkrete Ausprägung der genannten Globalanforderungen – Vertraulichkeit, Integrität, Verfügbarkeit und Verbindlichkeit – im Einzelfall festzustellen. Nur wenn klar definiert ist, welche Leistungen des IT-Systems in welcher Weise verfügbar sein müssen, und welche Daten, Anwendungen oder Prozesse in welcher Hinsicht vertraulich und/oder integer, d. h. unverfälscht, sein müssen, können gegen das System wirksame Risiken identifiziert und im Weiteren durch geeignete Maßnahmen eliminiert werden.

Standards

Der Aufwand zur Erstellung und Pflege eines IT-Sicherheitskonzepts lässt sich deutlich reduzieren, wenn standardisierte Komponenten eingesetzt werden können und so auf dafür vorhandene Maßnahmen und Risikoanalysen zurückgegriffen werden kann. Dazu wird im Schritt der **Modellierung** eine Abbildung der vorhandenen realen Strukturen auf standardisierte Elemente vorgenommen. Dazu stützt man sich auf etablierte Kataloge von Schutzmaßnahmen und Gefährdungsanalysen ab. Hier sind im zivilen Bereich die Normen ISO 27001, ISO 17799 und ISO TR 13335 sowie die IT-Grundschutzkataloge des BSI und im militärischen Umfeld vor allem die Vorschrift ZDv 54/100 einschlägig.

Die Betrachtung dieser standardisierten Komponenten liefert umfassende und praxisorientierte Hinweise auf konkrete **Schwachstellen** und die zu ihrer Abdeckung notwendigen Schutzmaßnahmen. Die Analyse der bisher getroffenen Schutzmaßnahmen schließt die Untersuchung aller relevanten technischen, organisatorischen, infrastrukturellen und personellen Vorkehrungen, die den Eintritt bzw. die möglichen Auswirkungen der betrachteten Risiken zu vermeiden helfen.

Umsetzung

Zur Reduzierung bzw. Beseitigung der festgestellten Schwachstellen erfolgt eine **Maßnahmenplanung**, die sich ebenfalls weitgehend auf die standardisierten Kataloge abstützen kann. Dabei ist davon auszugehen, dass bestimmte Maßnahmen als unverzichtbare Basis auf jeden Fall ergriffen werden sollten, um so zu verhindern, dass nicht tragbare Risiken auf vorhandene Schwachstellen wirken. Eine weitere Analyse der Risikosituation, eine Auswahl sonstiger Maßnahmen und deren Bewertung kann in der Regel entfallen, wenn die Schutzbedarfsfeststellung keinen hohen oder sehr hohen Schutzbedarf ergeben hat. In diesem Fall erübrigen sich dann alle späteren und aufwendigen Untersuchungen.

Eine detaillierte **Risikoanalyse** kann sich bei diesem Vorgehen auf zwei Problembereiche beschränken:

- Anwendungen bzw. Daten, für die ein erhöhter Schutzbedarf festgestellt wurde, können die Installation weiterer Schutzmaßnahmen erfordern.
- Spezielle Lücken, die bei der Untersuchung der vorhandenen Infrastruktur und der sich aus den Vorschriften ergebenden organisatorischen, personellen und technischen Maßnahmen festgestellt werden, müssen durch geeignete zusätzliche Schutzmaßnahmen geschlossen werden. Ebenso sind spezifische Bedrohungen, die sich aus der Anwendung der IT im Einzelfall ergeben können, durch diesen Bedrohungen angepasste Schutzmaßnahmen abzusichern.

Diese Gefährdungsübersicht wird systematisch abgearbeitet, d. h. für jedes Zielobjekt und jede Gefährdung wird geprüft, ob die bereits umgesetzten oder zumindest im IT-Sicherheitskonzept vorgesehenen IT-Sicherheitsmaßnahmen einen ausreichenden Schutz bieten. Anhand der verbleibenden Gefährdungen muss für jedes noch bestehende *Risiko* eine Entscheidung getroffen werden, ob es durch weitere Schutzmaßnahmen wirtschaftlich vertretbar abgewehrt werden kann, durch Umstrukturierung der IT vermieden oder ob es als Restrisiko akzeptiert werden soll.

Kontrolle und Pflege

Die kontinuierliche **Fortschreibung** des IT-Sicherheitskonzepts (z. B. durch Austausch von System- oder Programmkomponenten in einem IT-Verfahren) ist in der Regel mit einem nicht unerheblichen Arbeitsaufwand verbunden. Es besteht auch die Gefahr, dass dabei einzelne Bereiche der IT-Sicherheit übersehen, falsch eingeordnet oder inkonsistent erfasst werden. Die Menge der Informationen in einem typischen IT-Sicherheitskonzept macht es sehr schwierig, derartige Inkonsistenzen und Lücken zuverlässig zu erkennen und zu vermeiden.

Durch Einsatz eines geeigneten **Werkzeugs** können sowohl die angewendeten Methoden vollständig und standardkonform umgesetzt werden und auch die Konsistenz und Aktualität der erfassten Informationen sicher gestellt werden. Überarbeitungen können mit deutlich reduziertem Aufwand vorgenommen werden. Die auf dem Markt angebotenen Werkzeuge basieren im allgemeinen auf Datenbanken, die die zu beachtenden Maßnahmen und Gefährdungen sowie die Beziehungen untereinander enthalten. Durch die direkte Unterstützung einer vorgegebenen Methodik wird der Benutzer zu den einzelnen Schritten hingeführt, die er zum Aufbau und zur Pflege des IT-Sicherheitskonzepts umzusetzen hat.

Wenn auch die Nutzung derartiger Werkzeuge zur Erstellung eines IT-Sicherheitskonzepts für wenig komplexe Systemumgebungen nicht zwingend notwendig ist, so wird diese Aufgabe dadurch doch häufig deutlich erleichtert. Sofern aufgrund größerer Komplexität und mehrschichtiger Anforderungen eine Kombination geeigneter Methoden angezeigt ist oder aufgrund der Sicherheitsanforderungen eine Risikoanalyse erforderlich ist, kann auf den Einsatz eines geeigneten Werkzeugs kaum noch verzichtet werden. Im Rahmen einer **Wirkungsnetzanalyse** können so Zusammenhänge und Querbeziehungen zwischen Schutzobjekten, Maßnahmen und Gefährdungen abgebildet und analysiert werden, was manuell nicht mehr konsistent erstellt und gepflegt werden könnte. Eine deutliche Effizienzsteigerung erzielt der Werkzeugeinsatz im Rahmen von Kontrollen und Audits des IT-Sicherheitsprozesses bis hin zur Durchführung von Zertifizierungen.

Über die INFODAS GmbH

INFODAS gehört zu den innovativen deutschen mittelständischen Systemhäusern für Sicherheitslösungen und Risikomanagement. BSI-lizenzierte IT-Grundschutz- sowie ISO 27001-Auditoren der INFODAS führen ganzheitliche IT-Sicherheits-Beratungen auf Basis der IT-Sicherheitsdatenbank SAVE[®] durch, konzipieren und auditieren Organisationen und IT-Sicherheitsprozesse. INFODAS entwickelt geeignete Notfallvorsorge-Programme, gestaltet und überprüft den Datenschutz und stellt externe Datenschutzbeauftragte zur Verfügung.

SAVE[®] bietet als Ergänzung zum Grundschutz eine Verfahrenshilfe für die Umsetzung des Datenschutzes und der Datensicherheit an. Für die militärische Nutzung von SAVE[®] ist eine Implementierung der ZDv 54/100 verfügbar.

INFODAS hat u.a. die Auditierungen der IT-Grundschutz-Zertifikate der „SAP Systems Integration AG“ und der „TDS Informationstechnologie AG“ geplant und erfolgreich und schnell ausgeführt. Mit der „BOGESTRA – Bochum Gelsenkirchener Straßenbahnen AG“ wurde die erste ISO 27001-Zertifizierung auf der Basis von IT-Grundschutz abgeschlossen. INFODAS arbeitet langjährig erfolgreich mit dem BSI bei Anwendung und Fortschreibung des IT-Grundschutzhandbuchs zusammen.

Ein auf der Sicherheitskonzeption aufbauendes Risikomanagement und -controlling unterstützt die Anforderungen des KonTraG und die Vorgaben von BASEL II.

Ansprechpartner:

Frank Reiländer
Leiter Business Unit IT Security
Tel.: (0221) 7 09 12-85
Fax: (0221) 7 09 12-55
Email: F.Reilaender@infodas.de

Pressekontakt

Eva Wagenbach
möller pr
Tel.: (0221) 80 10 87- 88
Mobil: (0174) 980 1375
Email: ew@moeller-pr.de

INFODAS GmbH
Gesellschaft für Systementwicklung und
Informationsverarbeitung mbH
Rhonestraße 2
D-50765 Köln

<http://www.save-infodas.de/>