VICARDION®

IT Security Management

So erreichen Sie systematisch bereichsübergreifend ein optimales Sicherheitsniveau

VICARDION GbR
Karl-Wirth-Str. 10
76694 Forst

+49 (0) 7251 32658 0
info@vicardion.de
www.vicardion.de

Autor(en): Eduard Schwab
Stand: Oktober 2022
Version: 2.0.1

Inhaltsverzeichnis

Vorwort

Der Bedarf an Sicherheit in der Informationstechnologie nimmt stetig zu und das nicht ohne Grund. Sich ständig ändernde IT-Umgebungen und neuste Technologien bringen neue Chancen aber auch Risiken mit. Zunehmende Mobilität sowie die Nutzung von Online Diensten führen zur Auflösung der Grenzen eines genau definierten IT-Verbunds. Empfindliche Unternehmensdaten können von jedem Ort mit beliebigem Gerät abgerufen, bearbeitet und praktisch überall abgelegt werden. Unternehmen jeder Größe, Institutionen und deren Sicherheitsverantwortliche sehen sich zunehmend vor neuen Herausforderungen, müssen immer mehr auch gesetzliche Aspekte beachten, flexibel sein und gleichzeitig schnell, gezielt und individuell reagieren.

Für diese herausfordernden Aufgaben wird ein Werkzeug oder besser ein System benötigt, welches die Sicherheitsverantwortlichen bei Ihrer Arbeit unterstützen kann.

Lesen Sie was wir unter IT Security Management verstehen, was sich im Detail dahinter verbirgt und wie Unternehmen und Institutionen davon profitieren können.

Auch wenn wir uns in diesem Dokument am IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik) orientieren, sei bereits an dieser Stelle erwähnt, dass es nicht die einzige Möglichkeit ist ein wirksames Informations-Sicherheitsmanagement System (ISMS) aufzubauen und zu betreiben.

IT Security Management

Aufgrund der im Vorwort erwähnten Herausforderungen reicht es in der heutigen Zeit nicht mehr aus einen Virenscanner und eine Firewall einzusetzen und sich sicher zu fühlen. Doch welche Maßnahmen müssen ergriffen werden? Welche Bereiche sind besonders schützenswert? Welchen Risiken ist ein Unternehmen überhaupt ausgesetzt und welche Folgen kann das Eintreten eines Risikos haben?

Die Antworten auf diese Fragen liefert das IT Security Management. IT Security Management ist ein Prozess, der IT-Sicherheitsverantwortliche dabei unterstützt alle Herausforderungen zu überblicken und relativ schnell ein gewisses Maß an Sicherheit zu erreichen.

Dieses Dokument orientiert sich am IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik). Der IT-Grundschutz verfolgt u.a. das Ziel ganz individuell mit möglichst wenig Aufwand (was sich natürlich direkt auf die Kosten auswirkt) ein möglichst hohes Maß an Sicherheit zu erreichen und einen Prozess zu erschaffen, welcher dauerhaft ein vernünftiges Sicherheitsniveau gewährleistet.

Systematische Zielerreichung

Der Anfang

Im Grunde kann man sagen, dass IT Security Management von der Geschäftsleitung angestoßen und vorgelebt werden muss. Das Management muss erkennen und allen im Unternehmen deutlich machen, dass IT Security und Datenschutz wichtige und sensible Themen sind. Nicht unbedeutend sind an dieser Stelle die gesetzlichen Vorschriften die es einzuhalten gilt, aber auch das Haftungsrisiko des Unternehmers. Um einen IT Security Prozess aufzubauen, muss ein Verantwortlicher also ein IT Security Beauftragter benannt werden. Optimal wäre ein mehrköpfiges Security-Team, in das so viele Abteilungen wie möglich eingebunden sind. IT Security muss einen Platz in der Unternehmenspolitik einnehmen und somit eine Basis für ein IT Security Management bilden.

Gefährdung analysieren

Es muss an Hand der Geschäftsprozesse festgestellt werden mit welchen Daten und mit welchen Systemen im Unternehmen bzw. in der Institution gearbeitet wird. Welche Systeme und Daten sind erforderlich, um den Geschäftsbetrieb aufrecht zu erhalten. Weiß man erst welche Daten von welchen Systemen bearbeitet werden, kann man, unter Berücksichtigung gesetzlicher Vorschriften, ein erforderliches Sicherheitsniveau bestimmen und in Sicherheitsleitlinien festhalten. Es gilt die **Verletzbarkeit** des eigenen Unternehmens in Bezug auf mögliche Bedrohungen abzuwägen.

Verletzbarkeit

Ein Unternehmen bzw. eine Institution ist in Bezug auf die **Verfügbarkeit, Vertraulichkeit** und **Integrität** ihrer Daten verletzbar. Kann z.B. die Verfügbarkeit, Vertraulichkeit und Integrität der Daten nicht mehr sichergestellt werden so spricht man von Verletzbarkeit.

Bedrohungen

Die Verletzbarkeit steht wiederum gewissen Bedrohungen gegenüber. Dazu gehören:

- **Menschliche Fehlhandlungen**
- **Technisches Versagen**
- **Vorsätzliche Handlungen Dritter**
- **Organisatorische Mängel**
- **Höhere Gewalt**

Nach erfolgter Gegenüberstellung der Verletzbarkeit und den Bedrohungen spricht man unter Berücksichtigung der Eintrittswahrscheinlichkeit von einem Risiko.

Verletzbarkeit + Bedrohungen = Risiko

Gegenmaßnahmen

Einem Risiko kann man mit dem Ergreifen bestimmter Maßnahmen entgegenwirken. Die zu ergreifenden Maßnahmen sind nicht nur technischer, sondern sehr stark auch organisatorischer Natur. Unterschiedliche Statistiken besagen, dass die Ursachen für Schäden in der IT mit rund 70% menschlichen Fehlhandlungen und physischen Ereignissen zuzuordnen sind. Spätestens an dieser Stelle, sollte der ganzheitliche Ansatz des IT Security Managements deutlich werden.

Maßnahmen können für folgende Bereiche ergriffen werden:

- **Infrastruktur**
- **Personal**
- **Organisation**
- **Hardware und Software**
- **Kommunikation**
- **Notfallkonzepte**

Die Unternehmensleit- und Richtlinien unterstreichen u.a. die Wichtigkeit von einem Sicherheitsprozess, verdeutlichen die Haltung des Managements zum Thema IT-Sicherheit und begründen die Erstellung und Einführung eines Sicherheitsprozesses.

Sicherheitskonzept

Ist man sich über die Verletzbarkeit, möglichen Bedrohungen und empfindlichsten Bereiche seiner Organisation im Klaren, muss ein Sicherheitskonzept entwickelt werden. Hierzu müssen wesentliche Schritte und Regeln eingehalten werden, die detaillierte Informationen, wichtige Aufschlüsse und vielleicht sogar überraschende Ergebnisse liefern können.

IT-Strukturanalyse

In der Strukturanalyse werden Daten erhoben, die für die Erstellung des IT-Sicherheitskonzepts von Bedeutung sind. Diese Daten werden übersichtlich und strukturiert, zur weiteren - vorerst abstrakten - Betrachtung aufbereitet. Spätestens nach der IT-Strukturanalyse wird die IST-Situation klar. Es wird deutlich, welche Komponenten vorhanden sind, welche Applikationen verwendet werden und welche Zusammenhänge bestehen.

Ermittlung des Schutzbedarfs

In dieser Phase werden die Anwendungen und Systeme im Hinblick auf die Vertraulichkeit, Verfügbarkeit und Integrität unter Berücksichtigung der zuvor ermittelten Abhängigkeiten, bewertet und in Schutzbedarfskategorien eingeteilt. Je nach Schadenswahrscheinlichkeit und Bedeutung der einzelnen Bereiche müssen entsprechend einfache oder aufwändige Sicherheitsmaßnahmen ergriffen werden.

Modellierung

Die Modellierung verfolgt das Ziel die erforderlichen Sicherheitsmaßnahmen zu bestimmen. Hierfür werden einzelnen Komponenten den, für die IT-Sicherheit empfohlenen bzw. vorgeschriebenen, Sicherheitsmaßnahmen gegenübergestellt. Gleichzeitig kann überprüft werden welche Maßnahmen bereits umgesetzt sind.

Zusätzliche Sicherheitsanalysen

Für sehr empfindliche und kritische Bereiche mit hohem bzw. sehr hohem Schutzbedarf müssen ergänzende Sicherheitsanalysen durchgeführt werden. Diese Bereiche müssen separat

beleuchtet und mit zusätzlichen Maßnahmen über eine Grundabsicherung hinaus geschützt werden.

Sicherheitscheck

Im sogenannten Basis-Sicherheitscheck werden bereits vorhandene Sicherheitsmaßnahmen überprüft, d.h. es wird ein Soll-/Ist-Vergleich angestellt. Die Abweichung zu den empfohlenen Maßnahmen wird festgehalten und fließt in den Realisierungsplan mit ein.

Die Auseinandersetzung mit der IT-Struktur, die Feststellung des Schutzbedarfs, die Modellierung und der Sicherheitscheck führen letztendlich zu einer individuellen Handlungsanleitung, also einem Sicherheitskonzept.

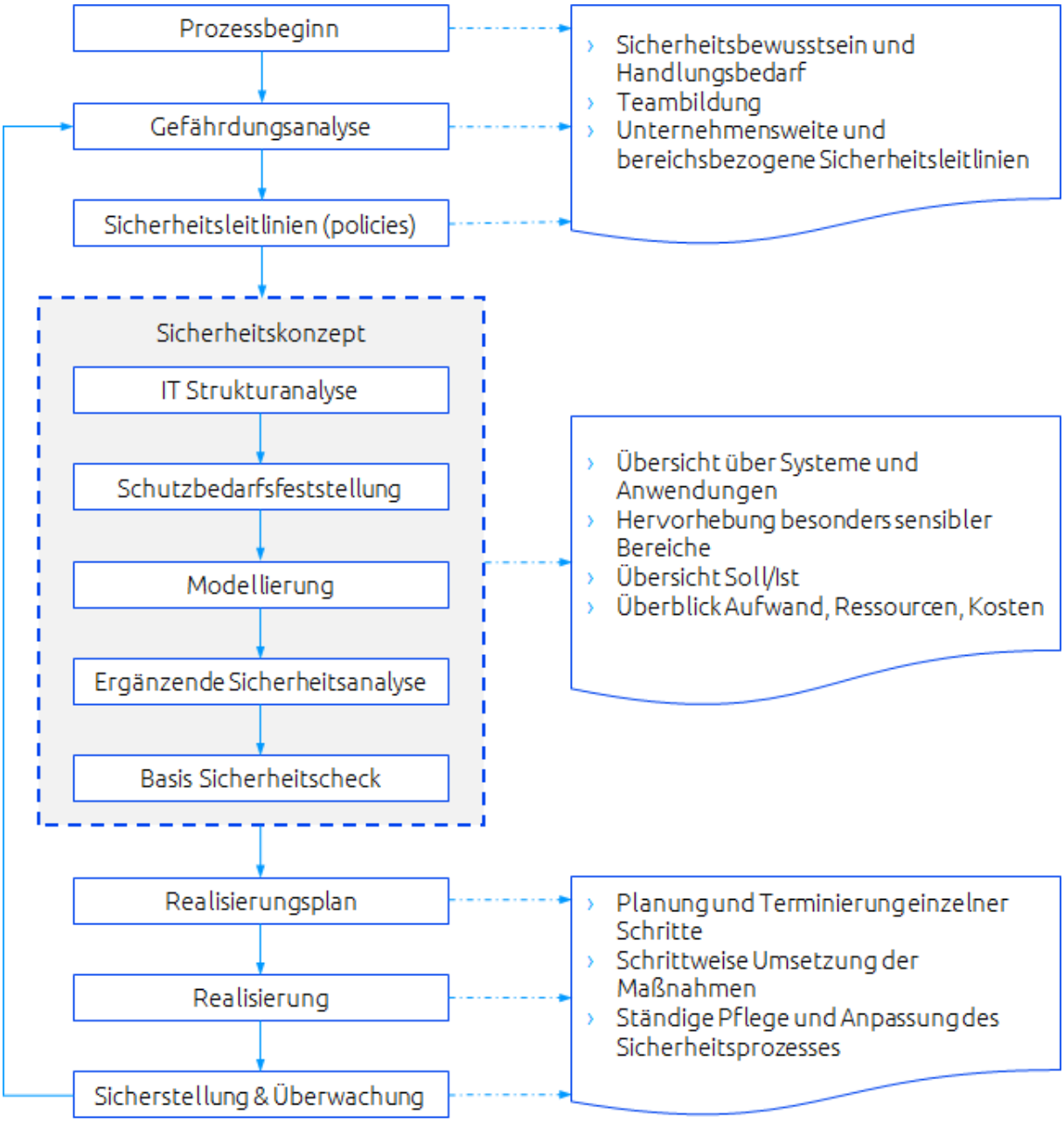
Planung, Realisierung und Monitoring

Steht erst mal ein Konzept geht es an die eigentliche Arbeit, also an die Umsetzung. Hier wird die Realisierung geplant, indem z.B. Zuständigkeiten und Termine festgelegt werden. Sobald das Sicherheitskonzept umgesetzt ist, muss dieses Konzept im Betrieb sichergestellt und gelebt werden. Bei wechselnden Anforderungen und Modernisierungen muss das Sicherheitskonzept u.U. erweitert und angepasst werden.

Wenn ein IT Security Konzept entwickelt und ein IT Security Prozess erfolgreich eingeführt wurde, bietet es sich an eine Zertifizierung nach ISO 27001 durchzuführen. Dies bringt für viele Unternehmen weitere Vorteile für die Kreditwürdigkeit, im Wettbewerb aber auch Imagevorteile mit.

IT Security Prozess

Die folgende Abbildung soll zur Verdeutlichung den zuvor beschriebenen IT Security Prozess grafisch darstellen.



Für wen ist IT Security Management geeignet?

IT Security Management ist für alle Unternehmen, öffentliche Einrichtungen, Institutionen und Organisationen jeder Art geeignet, die an einer Sicherheit ihrer Daten und Informationstechnologie interessiert sind.

IT Security Management beinhaltet einen Sicherheitsprozess, welcher sich wiederum auf ein Sicherheitskonzept stützt.

IT Security Management ist unabhängig von der Größe einer Organisation, verschafft in einem ganzheitlichen Ansatz einen Überblick, beantwortet viele Fragen, führt zu einem individuellen Sicherheitskonzept und verfolgt das Ziel mit möglichst wenig Aufwand ein gesundes Maß an Sicherheit zu erreichen.

Unternehmen und Institutionen die mit besonders empfindlichen Daten agieren unterliegen im besonderen Maße zusätzlich gesetzlichen Schutzbestimmungen. Weiterhin gibt es Branchen und Organisationen für die eine nachweislich umgesetzte IT-Sicherheit wichtige Wettbewerbsvorteile einbringt. Für diese Unternehmen und Institutionen wird IT Security Management zu einem sehr wertvollen Instrument. Hat ein Unternehmen oder eine Institution erst ein Sicherheitsprozess etabliert und alle benötigten Maßnahmen erfolgreich umgesetzt, kann dieses Unternehmen nach ISO 27001nativ oder auf Basis des IT-Grundschutzes, bei einer anerkannten Zertifizierungsstelle, zertifiziert werden.

Vorteile

- Kosteneinsparung durch gezielte Schutzmaßnahmen
- Positive Auswirkungen auf die Haftung und Kreditwürdigkeit
- Ganzheitlicher Lösungsansatz
- Systematische und abstrakte Betrachtung Ihres IT-Verbundes
- Flexible und exemplarische Betrachtung besonders kritischer Geschäftsbereiche
- Unternehmens-/institutionsbezogener IT-Schutz
- Bedarfsgerechter Schutz sensibler Unternehmensdaten
- Ganzheitlicher Schutz der IT-Infrastruktur
- Basis für die ISO 27001 Zertifizierung
- Erfüllung gesetzlicher Vorschriften

Zusammenfassung

Lässt man im eigenen Haus alle Garagentore, Türen sowie Fenster offen und die wertvollsten Unterlagen und Gegenstände mitten im Zimmer auf dem Tisch liegen, provoziert man fahrlässig große Unannehmlichkeiten und erhöht das Risiko, dass etwas gestohlen wird.

Schließt man dagegen alle Fenster, Türen sowie Tore ab und räumt die Unterlagen und Wertgegenstände weg, hat man mit relativ wenig Aufwand ein vernünftiges Maß an Sicherheit erreicht. Besonders schützenswerte Sachen würde man entweder zu einer Bank bringen oder zusätzliche Sicherheitsmaßnahmen treffen. Je nach Schutzbedarf würde man die Sachen im Tresor aufbewahren, Sicherheitstüren und -Fenster einbauen, eine Alarmanlage oder gar eine Videoüberwachung installieren.

Genauso verhält es sich mit der IT-Sicherheit, wobei das IT Security Management uns bei der Wahl der richtigen Maßnahmen unterstützt.