INTARGIA

In Kooperation mit

Deutsche Leasing

> **> Hier erfahren Sie, ...**

... warum IT-Sicherheit in allen Unternehmens-bereichen unerlässlich ist

... was Pflicht ist und wie Sie den Aufwand im Rahmen halten

... wie IT-Sicherheit dauerhaft und nachhaltig gesichert wird

IT-Sicherheit für das ganze Unternehmen

Leitfaden für die Praxis

IT-Sicherheit für das ganze Unternehmen

Leitfaden für die Praxis

Inhalt

Teil 1 Wissen

IT-Sicherheit betrifft alle

Eine Vielzahl von Faktoren wie die zunehmende Verbreitung von Internet-Anwendungen, die Integration von Systemen über Unternehmensgrenzen hinaus, der wachsende Einsatz drahtloser Technologien oder die Flut neuer gesetzlicher Regelungen machen „Sicherheit" zu einem der zentralen Themen auf der Agenda von IT-Verantwortlichen. Fallen IT-Systeme aus, dann stört das Geschäftsabläufe in der Regel existentiell. Die Produktion steht still, Kunden warten auf Auskunft, Rechnungen werden nicht geschrieben. Die Bedeutung von IT-Sicherheit ist in Unternehmen bekannt, über die exakten Folgen und Folgekosten von Sicherheitsmängeln jedoch herrscht häufig Unklarheit. Sie beginnen beim Ärger über volle E-Mail-Postfächer und enden bei der persönlichen Haftung von Vorständen und Geschäftsführern. Hinter dem Begriff IT-Sicherheit verbergen sich Maßnahmen und Lösungen zum Schutz Ihrer IT-Systeme vor Störungen, Ausfall, Sabotage, Manipulation und unerlaubtem Zugriff. Übergeordnetes Ziel dabei ist stets die Sicherung der Arbeitsfähigkeit des Unternehmens. Je nach Grad der Sicherheitsbedürfnisse sind mit der Gewährleistung von IT-Sicherheit zum Teil erhebliche Kosten verbunden. Gefragt ist die perfekte Balance zwischen betrieblichen und rechtlichen Notwendigkeiten einerseits und dem wirtschaftlich Sinnvollen andererseits. Hierfür sind abgestufte Konzepte zu entwickeln, welche die Folgen möglicher Sicherheitslücken in allen Bereichen aufzeigen, Gegenmaßnahmen ermitteln, Kosten und Nutzen bewerten und darauf basierend konkrete Maßnahmen festlegen.

Wo lauern Risiken und Gefahren?

Die Bedrohungen für IT sind vielfältig. Sie entstehen durch „Angriffe" von außen, sehr viel häufiger aber durch die eigenen Mitarbeiter im Unternehmen. Zumeist unbewusst und ohne böse Absicht werden von Anwendern Viren eingeschleppt, Passwörter weitergegeben oder Datensicherungen unterlassen. Datenverluste, unerlaubte Zugriffe oder gar Systemausfälle sind die Folgen. Vielfach aber sind nicht die Anwender schuld an Sicherheitslücken, sondern die IT-Verantwortlichen selbst. Fehlende oder nicht aktuelle Sicherheitskonzepte, nicht ausreichende Ressourcen für das Sicherheitsmanagement,

Info 1 2 3 4 5 6

Strategie und klare Ziele zur IT-Sicherheit sind die Basis zum Einstieg in einen dauerhaften Prozess.

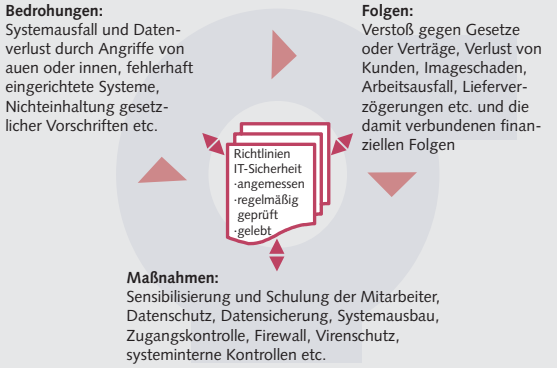
Info 1 2 3 4 5 6

Die Kommunikation klarer Regeln spielt bei der Überzeugung der Mitarbeiter eine entscheidende Rolle.

veraltete Hard- und Softwareprodukte zur System- und Netzwerkadministration oder schlicht Mängel in den Verfahrensanweisungen zur IT-Sicherheit – die Liste der in der Praxis zu beobachtenden Versäumnisse ist lang. Häufig nicht bekannt sind die Haftungsregeln, denen IT-Verantwortliche, aber auch Vorstände bzw. Geschäftsführungen für Versäumnisse im Bereich IT-Sicherheit unterliegen.

Eine diesbezügliche „Matrix der Haftungsrisiken" hat der Verband BITKOM* herausgegeben.

Abb. 1 **IT-Sicherheit richtig bewerten**



* Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V., www.bitkom.org

Teil 2 Projekt IT-Sicherheit

Prioritäten richtig setzen

Der tatsächliche Schutzbedarf ist der einzig sinnvolle Ausgangspunkt zur Konzeption und Umsetzung von IT-Sicherheitsmaßnahmen. Nur so ist die Ausgewogenheit von Aufwand und Nutzen sicherzustellen. Ein geeignetes Hilfsmittel zur Ermittlung der Prioritäten ist die Definition von Schutzkategorien – niedrig, mittel, hoch, sehr hoch. Betrachten Sie jede mögliche Bedrohung unter dem Aspekt möglicher Schadensszenarien wie

- komplette oder teilweise Betriebsausfälle
- finanzielle Risiken
- Verstoß gegen gesetzliche Vorschriften oder Verträge
- Verletzung der Persönlichkeitsrechte
- negative Außenwirkung

Schritt für Schritt

Phase 1: Vorbereitung

Streng genommen ist IT-Sicherheit kein Projekt. Der Schutz der IT-Systeme ist ein dauerhafter Prozess. Dennoch ist ein Projekt der beste Weg zum Einstieg in IT-Sicherheit oder die grundlegende Prüfung, Konsolidierung und Neuausrichtung Ihrer Aktivitäten in diesem Feld. Grundlage ist eine auf Ihre geschäftlichen Ziele ausgerichtete Sicherheitsleitlinie.

Stellen Sie sich mindestens folgende Fragen:

- Bei welchen Geschäftsprozessen können Sie sich Ausfälle von unterstützenden IT-Systemen oder von Informationen keinesfalls erlauben?
- Wie lange sind Sie ohne diese Informationen arbeitsfähig?

Info 1 2 3 4 5 6

Die Integration von mobilen Technologien stellt auch neue Herausforderungen an IT-Sicherheit.

Info 1 2 3 4 5 6

Bewerten Sie jede Sicherheitsmaßnahme nach Kosten und Nutzen im jeweiligen Schadenfall.

- Was passiert, wenn Informationen vollständig verloren sind?
- Welche Risiken sind tragbar, welche nicht?
- Kann der Systemausfall mit Behelfslösungen, notfalls manuell, kompensiert werden?

Auf dieser Basis können Sie die Projektziele festlegen.

Wesentliche Rahmenbedingung für das Gelingen eines Projektes „IT-Sicherheit" ist die frühzeitige Einbindung wichtiger Beteiligter aus Geschäftsführung, Personalmanagement, Betriebsrat und IT sowie eines Datenschutzbeauftragten. Die Rolle des verantwortlichen Entscheiders (nicht des operativ im Projekt Verantwortlichen) kann sowohl der IT-Leiter als auch z.B. der Datenschutzbeauftragte übernehmen. Vorstand bzw. Geschäftsführung müssen in einem Lenkungsausschuss vertreten sein oder regelmäßig über den Status informiert werden. Das ergibt sich bereits aus der im Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)* geforderten Pflicht zum unternehmensweiten Risikomanagement, die auch IT-Risiken umfasst.

Phase 2: Ist-Analyse der IT-Struktur

Zur Planung der für Ihr Unternehmen optimalen Sicherheitslösungen ist zunächst ein umfassender Blick in die bestehende IT-Landschaft erforderlich. Dabei werden alle vernetzten und nicht vernetzten Systeme aus dem Blickwinkel „Sicherheit" analysiert. Zusätzlich zur Funktion einzelner Komponenten in der Gesamtarchitektur spielen die Kommunikationsverbindungen zwischen den Systemen und mit der Außenwelt eine wichtige Rolle. Die Verfügbarkeit von geschäftsrelevanten Informationen ist ein wesentlicher Baustein der IT-Sicherheit. Daher spielt die Datensicherung eine wichtige Rolle. Typische Fragen sind:

- Wie und wie oft werden Daten gesichert?
- Gibt es ein Datenarchiv?
- Können Daten/Informationen nach Problemfällen konsistent wiederhergestellt werden?

Mit der Zunahme von mobilen Verbindungen via Laptop, PDA und drahtlos per Funk rücken auch die organisatorischen und personellen Rahmenbedingungen in den Fokus.

- Wer darf von wo auf Systeme und Anwendungen mit welchen Rechten zugreifen ?
- Welche Authentisierungsmechanismen werden genutzt?
- Wie werden Passwörter gemanagt?
- Kommen Signaturen oder gar biometrische Verfahren zum Einsatz?

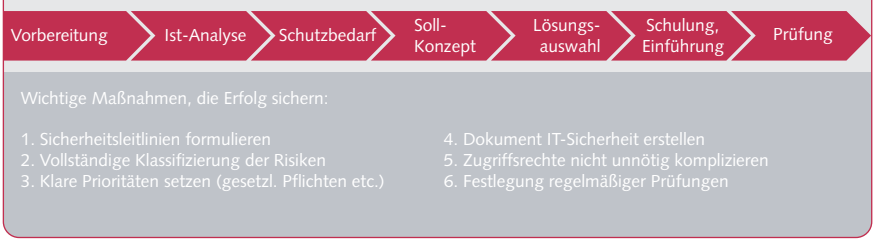
Ergebnis der gesamten Analyse ist eine umfassende „Landkarte" der Systeme, Zugangskontrollen und Schutzmechanismen.

Phase 3: Schutzbedarf feststellen

Mit der Festlegung Ihres tatsächlichen Schutzbedarfs bestimmen Sie maßgeblich auch die Höhe der notwendigen Budgets für IT-Sicherheit. Daher sollten Sie in dieser Phase sehr genau Risiken und Folgen durchdenken. Die Einordnung der Risiken in Schutzkategorien (niedrig, mittel, hoch, sehr hoch) liefert erste Anhaltspunkte zur Priorisierung späterer Maßnahmen. Wesentliche Kriterien für die Zuordnung in eine hohe Schutzstufe sind der Verstoß gegen gesetzliche Vorschriften oder Verträge,

* das Artikelgesetz KonTraG gilt seit Mai 1998 für Unternehmen mit mehr als 50 Mitarbeitern bzw. mehr als 6,87 Mio. Euro Umsatz

Abb. 2 **Der Weg zu wirtschaftlich angemesserer IT-Sicherheit**



die Verletzung von Persönlichkeitsrechten, die Beeinträchtigung der Aufgabenerfüllung, negative Außenwirkung und finanzielle Folgen. An der Erhebung, Verarbeitung, Speicherung, Verteilung und Löschung von Informationen sind eine Vielzahl von Mitarbeitern und eventuell sogar Externe beteiligt. Alle diese Akteure sollten Sie bei der Feststellung des Schutzbedarfs einbeziehen. Ermitteln Sie den konkreten Handlungsbedarf in einem mehrstufigen Prozess. Der ausgeprägte Wunsch, Informationen und Anwendungen möglichst immer und überall zugänglich zu haben, schwächt sich bei konkreter Nachfrage oft ab. So genannte „hochverfügbare Systeme“ mit einem Ausfallrisiko im Promillebereich erzeugen oft auch sehr hohe Kosten, bis hin zum Betrieb eigener Ausfallrechenzentren. Prüfen Sie sorgfältig, welcher Schaden tatsächlich eintreten könnte und ob es alternative nichttechnische Lösungen zum Umgang damit gibt.

Phase 4: Soll-Konzeption

Der ermittelte tatsächliche Schutzbedarf wird nun auf Basis der Leitlinien in ein Dokument zur unternehmensweiten IT-Sicherheit eingearbeitet. Eine solide Grundlage zur Erstellung ist das Schichtenmodell des Bundesamtes für Sicherheit in der Informationstechnologie (BSI). Dies teilt in die Bereiche:

- übergeordnete Aspekte (Organisation, Personal, Datensicherung, Virenschutz, Verschlüsselung etc.)
- Infrastruktur (Gebäude, Rechenzentrum, Serverraum etc.)
- IT-Systeme (PCs und andere Endgeräte, Netze und Netzwerkgeräte, Telearbeit etc.)
- Netz (System- und Netzmanagement, Modem, Firewall etc.)
- Anwendungen (Datenträger, Datenbanken, E-Mail etc.)

Das IT-Sicherheitskonzept ist ein Bekenntnis des Unternehmens zur IT-Sicherheit mit Wirkung nach innen und außen. Mitarbeiter sehen ihre Persönlichkeitsrechte geachtet, bei Partnern und Kunden schafft es Vertrauen in die Geschäftsabläufe. Dazu ist nicht unbedingt eine offizielle Zertifizierung notwendig. Grundsätzlich reicht z.B. ein Verweis auf die Einhaltung der Bestimmungen des IT-Grundschutzes gemäß BSI.

Phase 5: Auswahl & Realisierung

Eine komplette Lösung für Ihre individuelle IT-Sicherheit besteht in der Regel aus

- Hardwarekomponenten
- Softwarekomponenten
- Verfahrens- und Organisationsrichtlinien und -anweisungen

Der Markt für Hard- und Softwareangebote ist dynamisch und intransparent. Erfahrene Berater können Strategie- und Konzeptentwicklung, Vorselektion und Auswahlentscheidungen maßgeblich unterstützen.

Phase 6: Einführung & Schulung

Die Einführung einzelner Sicherheitskomponenten (z.B. die Auflösung oder Änderung von Dateiverzeichnissen oder neuen Backupsystemen) muss mit Trainings und Schulungen für das technische Personal und für weitere Mitarbeiter synchronisiert werden. Wichtig für eine nachhaltige Wirkung ist eine entsprechende Maßnahmenkommunikation, die sowohl notwendige Inhalte als auch die Philosophie, die hinter den Maßnahmen zur IT-Sicherheit steht, vermitteln muss.

Info 1 2 3 4 5 6

Deutsches Recht (KonTraG) verpflichtet zum unternehmensweiten Management von IT-Risiken.

Info 1 2 3 4 5 6

IT-Sicherheit muss regelmäßig überprüft und ggf. auf den Stand der Technik und Ihren Bedarf hin angepasst werden.

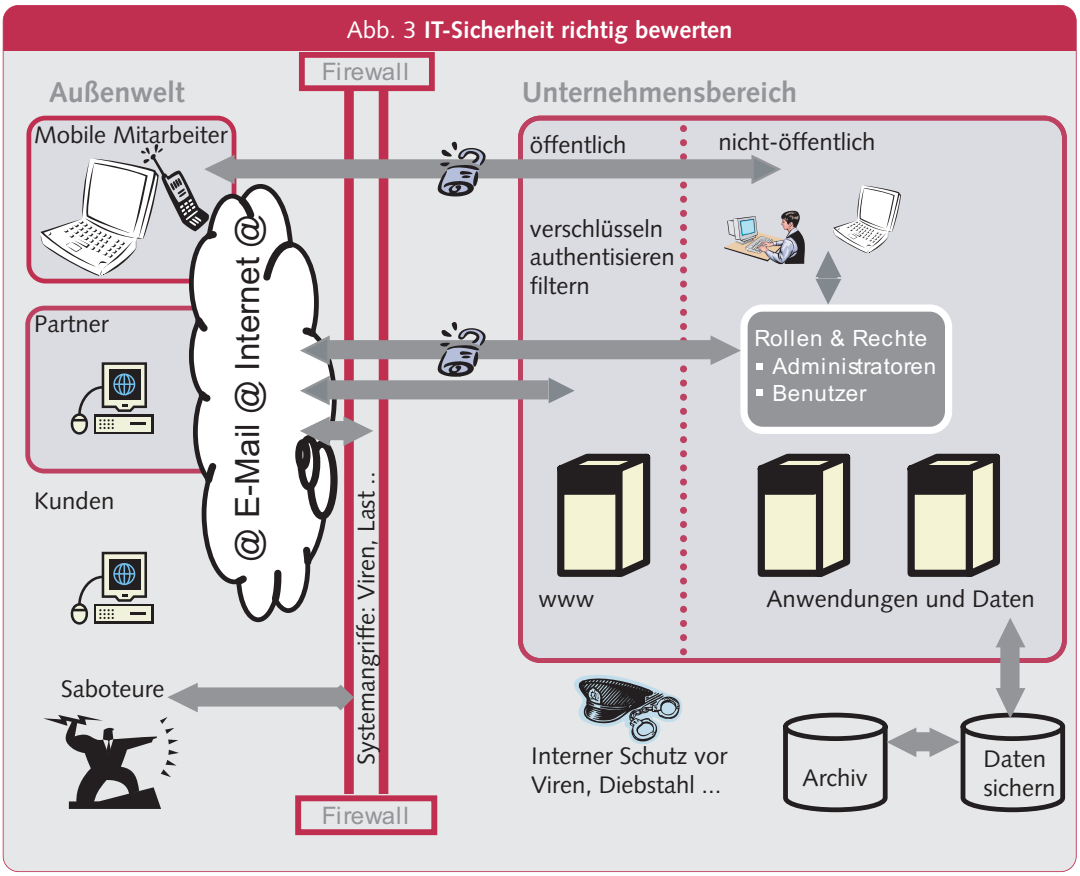
Phase 7: Fortlaufende Bewertung

IT-Sicherheit ist ein permanenter Prozess. Mit Abschluss des Projektes werden turnus- und routinemäßige Überprüfungen angestoßen. Wichtige Aspekte, die Anpassungen im Rahmen der IT-Sicherheit erfordern, sind vor allem die Veränderung der Bedrohungslage (z.B. auch gegeben durch unternehmerische Veränderungen wie internationales Wachstum oder Unternehmensübernahmen), gesetzliche Änderungen oder technologische Weiterentwicklungen.

Im Sinne größtmöglicher Nachhaltigkeit sollte auch die Option einer Zertifizierung geprüft werden. Standards wie ISO oder ITIL* decken das Thema IT-Sicherheit ab.

* Information Technology Infrastructure Library

Abb. 3 **IT-Sicherheit richtig bewerten**



✔ „Türsteher plus Polizeipatrouille“: Für die Sicherheit von Daten und Anwendungen werden zunehmend regelbasierte Firewalls mit internen Netzwerklösungen kombiniert. Firewalls verhindern das Eindringen in das lokale Netzwerk von außen (z.B. vom Internet) durch eine kontinuierliche Überwachung und Filterung des Datenverkehrs. Spezielle Software erkennt durch den Einsatz statistischer Verfahren sowie auf Basis bekannter Attacken die Bedrohungspotenziale im Innern.

✔ Zugangskontrollen werden mehr und mehr vereinheitlicht. Beim so genannten „Single Sign On“ reicht Nutzern eine Authentifizierung für alle Systeme. Mehrfache Passwortabfragen werden dadurch vermieden. Der größere Gewinn vereinheitlichter Zugänge liegt allerdings im deutlich sinkenden Aufwand zur Administration der Berechtigungen anhand von Rollen- und Rechtekonzepten.

✔ Ein vorrangiges Ziel bei der Verwirklichung von IT-Sicherheit ist es, durch notwendige IT-Maßnahmen die übrigen Betriebsabläufe nicht zu stören. Datensicherungen und Dateneinspielungen finden ebenso im laufenden Betrieb statt wie Releasewechsel und Software-Upgrades. Mit speziellen Verfahren kann erreicht werden, dass sich auch Virenscanner in Echtzeit aktualisieren und so schon kurz nach Bekanntwerden neuer „Schädlinge“ zur Verfügung stehen.

✔ Der Trend zur Auslagerung von IT-Sicherheitsleistungen bietet besonders mittelständischen Unternehmen Vorteile. Dies ist häufig wirtschaftlicher, da Ressourcen und Expertise nicht selbst vorgehalten werden müssen. Zudem ist eine Servicebereitschaft rund um die Uhr und an sieben Tagen der Woche mit angemessenem Aufwand erreichbar. Aber: Auch Auslagerungsprojekte („Outsourcing“) sind anspruchsvoll und bergen Risiken, denen angemessen begegnet werden muss.

✔ Für viele unbekannt ist, dass auch das Thema „Basel II“ mit IT-Sicherheit im Zusammenhang steht: Die Sicherheit der Geschäftsprozesse – und damit der IT-Systeme, auf denen sie laufen – ist ein wichtiges Kriterium zur Bewertung der Kreditwürdigkeit eines Unternehmens.

✔ Standards erleichtern den Umgang mit IT-Sicherheit. Gerüste wie ITIL oder COBIT, aber auch die Veröffentlichungen von Institutionen wie dem BSI oder dem Verband BITKOM helfen bei ersten Einschätzungen und der Planung konkreter Maßnahmen.

INTARGIA

In Kooperation mit

Deutsche Leasing

Die richtigen Kontakte für Ihre Projekte und eine auf Ihren Bedarf zugeschnittene Lösung

Strategische und operative Managementberatung:

INTARGIA Managementberatung
Max-Planck-Straße 20
D-63303 Dreieich
http://www.intargia.com

Ansprechpartner:
Dr. Thomas Jurisch
thomas.jurisch@intargia.com
Tel.: +49 6103 50 86-0

Finanzierung von IT-Projekten Leasing von Systemlösungen:

Deutsche Leasing AG
Frölingstraße 15 – 31
D-61352 Bad Homburg v. d. Höhe
http://www.deutsche-leasing.com

Ansprechpartner:
Holger Höhle, Angelika Zöller
holger.hoehle@deutsche-leasing.com
angelika.zoeller@deutsche-leasing.com
Tel.: +49 6172 88 22 54 / +49 6172 88 15 33