So verschafft sich die IT-Organisation Gehör

Angesichts der häufig mangelnden Sensibilität des Managements für IT-Risiken muss es dem IT-Chef gelingen, die Abhängigkeit des Unternehmens von der IT transparent zu machen.

Von **Holger Gerlach***

Ohne funktionierende IT-Systeme ist die Abwicklung von Geschäftsprozessen nicht mehr vorstellbar. Aufgrund der steigenden Abhängigkeit der Unternehmen von der IT hat sich IT-Sicherheit zum unternehmenskritischen Erfolgsfaktor entwickelt. Eine Erkenntnis, die allerdings häufig noch nicht in das Bewusstsein der Geschäftsleitung vorgedrungen ist. Gerade in wirtschaftlich schlechten Zeiten liegt es nahe, am IT-Budget zu sparen – im harten Gegensatz dazu verschärfen sich die Risikoszenarien im Umfeld der IT spürbar. Innerhalb dieses Spannungsfelds verbleiben wesentliche Sorgfaltspflichten beim IT-Verantwortlichen, der grundsätzlich vor zwei Herausforderungen steht. Für ihn gilt es zum einen, der Geschäftsleitung die Sicherheitsanforderungen verständlich zu machen, um Akzeptanz für notwendige Maßnahmen zu schaffen.

Für Akzeptanz sorgen

Zum anderen hat er im täglichen Betrieb dafür zu sorgen, dass die IT-Sicherheit in allen komplexen Teilbereichen ein angemessenes Niveau aufweist. Nur mit einem strukturierten und prozessbasierenden Vorgehen sind diese Aufgaben zu meistern.

IT-Anwendungen und -Systeme hielten über Jahrzehnte hinweg und in einem schleichenden Prozess Einzug in die Unternehmen. Aus diesem Grund entspricht die Sichtweise der Geschäftsleitung auf die IT nur selten dem Ist-Zustand, was dazu führt, dass reelle IT-Risiken allenfalls als virtuelle Bedrohungen für die eigene Organisation wahrgenommen werden. Erschwerend hinzu kommt die technische Komplexität der IT-Themen. Spätestens, wenn es um die Budgetgenehmigung für Sicherheitsmaßnahmen geht, wird der Dialog zwischen IT- und Geschäftsleitung schwierig. Argumentiert die IT-Abteilung mit typischen Angstszenarien, etwa Hacker-Angriffen oder Gesetzesverstößen, wird sie schnell als „Panikmacher“ oder „Verhinderer“ abgestempelt. Die Heraus-

Die Management-Sicht auf die IT entspricht selten dem Ist-Zustand.

forderung an dieser Stelle ist es, eine gemeinsame Kommunikationsbasis zu schaffen und der Geschäftsleitung die IT-Abhängigkeit des Unternehmens transparent zu machen. Es muss also gelingen, die Beeinträchtigung der IT als operationelles Unternehmensrisiko darzustellen. Der Fokus ist dabei nicht auf die möglichen Ursachen, sondern auf die potenziellen Auswirkungen zu legen. Das ist der erste Schritt auf dem Weg, die IT-Sicherheit in der Firmenstrategie zu verankern.

Die IT wird leicht als „Panikmacher" abgestempelt.

Um dieses Ziel zu erreichen, gilt es zunächst, in Zusammenarbeit mit der Geschäftsleitung die elementaren Geschäftsprozesse zu definieren und zu priorisieren. In einem nächsten Schritt werden diesen Abläufen unter Einbeziehung der jeweiligen Fachabteilungen alle benötigten IT-Anwendungen zugeordnet. Ausgehend von der Priorität des Prozesses wird dann der Schutzbedarf für die einzelnen Anwendungen und die damit verarbeiteten Daten eruiert.

Dabei gilt es, die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit zu bewerten. Besonders plakativ gegenüber der Geschäftsleitung wirken die oft hohen Anforderungen der Fachabteilungen an die Verfügbarkeit einzelner IT-Anwendungen. In diesem Schritt ist auch zu identifizieren und dokumentieren, ob bei der Datenverarbeitung rechtliche Belange wie etwa der Datenschutz tangiert werden.

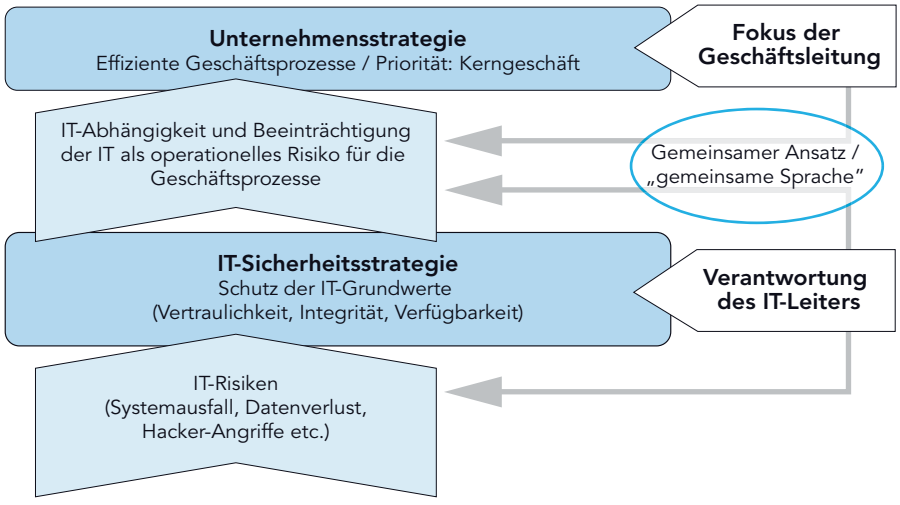
Foto: © Fotolia/Stephen Coburn

Auf Basis dieser Informationen lassen sich gegenüber der Geschäftsleitung fundierte Aussagen zum Stellenwert der IT im Unternehmen treffen. Indikator für die Abhängigkeit eines Geschäftsprozesses von der IT ist beispielsweise die Anzahl der benötigten Anwendungen in Verbindung mit dem geforderten Schutzbedarf für die jeweilige Anwendung.

Die daraus gewonnenen strategischen Erkenntnisse bezüglich der Priorität der IT im Unternehmen sowie das erforderliche Sicherheitsniveau sollten abschließend durch die Geschäftsleitung in einer „IT-Sicherheitsleitlinie" kommuniziert werden. Auf diese Weise signalisiert das Management einerseits sein Bewusstsein für den Stellenwert der IT und andererseits seine zentrale Verantwortung für die IT-Sicherheit. Die Verbindung zur Unternehmensstrategie ist somit hergestellt.

Eine gemeinsame Kommunikationsbasis schaffen

Die Beeinträchtigung der IT muss als operationelles Risiko für das Unternehmen dargestellt werden.



Quelle: OneConsult Deutschland

IT-Sicherheit als Prozess

Die für die beschriebenen Aufgaben erforderlichen Werkzeuge finden sich im Bereich IT-Sicherheits-Management, wo der gesamte Prozess – von der Planung, Umsetzung und Kontrolle bis hin zur Optimierung der IT-Sicherheit (PDCA-Modell) – geschaffen wird. Er besteht aus folgenden Schritten:

1. Zunächst gilt es, eine für die Größe des Unternehmens geeignete Organisationsstruktur zu etablieren. Eines der Hauptziele ist hier, klare Verantwortlichkeiten für die IT-Sicherheit (etwa Steuerung, Umsetzung, Prüfung) zu definieren.

Ein gemeinsamer Ansatz erleichtert den Dialog zwischen IT- und Geschäftsleitung.

2. Die dokumentarische Grundlage des Prozesses schafft die so genannte Strukturanalyse. Neben einem möglichst übersichtlichen Netzplan erfordert sie, alle IT-Anwendungen und -Systeme sowie Netzkomponenten inklusive deren Zusammenspiel zu erfassen. Umfang und Ausprägung der IT-Umgebung genau zu kennen ist Voraussetzung dafür, ▶

IT-Sicherheit – die Anforderungen

Konzeptionelle und technische IT-Sicherheitsanforderungen lassen sich in folgende Teilbereiche gliedern:

- **Organisatorische IT-Sicherheit:** In den Bereich Organisation fällt primär der Aufbau des IT-Sicherheits-Managements. Dabei sollte die Geschäftsführung zunächst eine IT-Sicherheitsleitlinie formulieren, die strategische Aussagen zur Priorität der IT und IT-Sicherheit enthält. Zudem müssen eindeutige Verantwortlichkeiten samt Vertretungsregelungen sowie Kommunikationswege definiert werden. Weitere Aufgaben sind, alle Maßnahmen und Veränderungen zu dokumentieren, die IT-Benutzer zu schulen und zu sensibilisieren sowie regelmäßige Audits (etwa Penetrationstests) vorzunehmen. An dieser Stelle entscheidet sich, ob IT-Sicherheit vom Management, den Administratoren sowie den IT-Benutzern als Prozess verstanden und gelebt wird.
- **Technische IT-Sicherheit:** Firewall, Virenscanner und Verschlüsselungssysteme sind wohl die gängigsten Beispiele für technische IT-Sicherheitsmaßnahmen. Aber auch Maßnahmen wie die Benutzerauthentifizierung mit Hilfe eines schlüssigen und umfassenden Rollen- und Rechtekonzepts sowie Netzsegmentierung und Systemhärtung fallen in diesen Bereich.
- **Physische IT-Sicherheit:** Vom Überschwemmungs- und Brandschutz über unterbrechungsfreie Stromversorgung und Klimatisierung bis hin zum Zutrittsschutz sowie dessen Überwachung – insbesondere beim Betrieb zentraler Server-Räume oder Rechenzentren kann der physische IT-Basisschutz mit erheblichem Aufwand verbunden sein. Ebenfalls zu berücksichtigen ist die sichere Entsorgung jeglicher Art von Datenträgern.
- **Betriebskonzepte:** Der sichere und stabile Betrieb einer IT-Umgebung setzt Konzepte für die Datensicherung, die geregelte Veränderung beziehungsweise Neuimplementierung von IT-Anwendungen sowie den Umgang mit Störungen voraus. Ebenfalls zu berücksichtigen sind das System- und Netz-Management sowie die Steuerung von Systemkapazitäten und -verfügbarkeiten. Die Bedeutung dieses Bereichs wächst mit der Größe der IT-Umgebung.
- **Notfallplanung:** Vollständige IT-Notfallpläne beinhalten neben Krisenstab und Alarmierungsplan vor allem Anleitungen zur Wiederherstellung kritischer IT-Anwendungen und -Systeme. Darüber hinaus sind die benötigte Verfügbarkeit der IT sowie die wahrscheinlichen Notfallszenarien zu definieren. Betreibt das Unternehmen ein Business-Continuity-Management, sind die Notfallpläne dort zu integrieren.
- **Vertragsbeziehungen:** Verträge mit externen Unternehmen müssen Verfügbarkeiten, Reaktions- und Behebungszeiten sowie die Verschwiegenheit einzelner Mitarbeiter verbindlich gewährleisten. Auch gesetzliche Aspekte wie die Anforderungen des Bundesdatenschutzgesetzes sind vertraglich abzudecken. Insbesondere beim Outsourcing von IT-Systemen sollte sich der Auftraggeber das Recht auf die Auditierung seines Partners einräumen lassen.
- **Wirtschaftlichkeit:** Neben der Wirksamkeit der IT-Sicherheitsmaßnahmen muss die IT-Abteilung auch nachweisen, dass diese angemessen sind. So gilt es, Aufwendungen etwa für sicherheitsspezifische Technik, Softwarelizenzen und Personal gegenüber Geschäftsführung und Fachabteilungen transparent zu machen. Existiert eine Kostenstellenrechung, muss die IT-Sicherheit dort entsprechend integriert werden.
- **Gesetzliche Anforderungen**: Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBs), Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU), Sarbanes-Oxley Act (SOX), Bundesdatenschutzgesetz (BDSG), Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) – die Liste von Gesetzen und Regulierungen mit direkten oder indirekten Auswirkungen auf die Firmen-IT wird von Jahr zu Jahr länger. Trotz unterschiedlicher Formulierung bleibt eine Anforderung gleich: die Pflicht, für fundierte IT-Sicherheit zu sorgen. Darüber hinaus sind verschiedene Ausprägungen zu beachten – etwa die Pflicht zur Archivierung von E-Mails (GDPdU), die Implementierung von Kontrollmechanismen (SOX) oder das Führen von Verfahrensverzeichnissen (BDSG).

schwachstellen zu ermitteln. Wie die Praxis zeigt, liegen diese Informationen – bedingt durch die Schnelllebigkeit der IT-Welt – oft nicht zentral und geordnet vor.

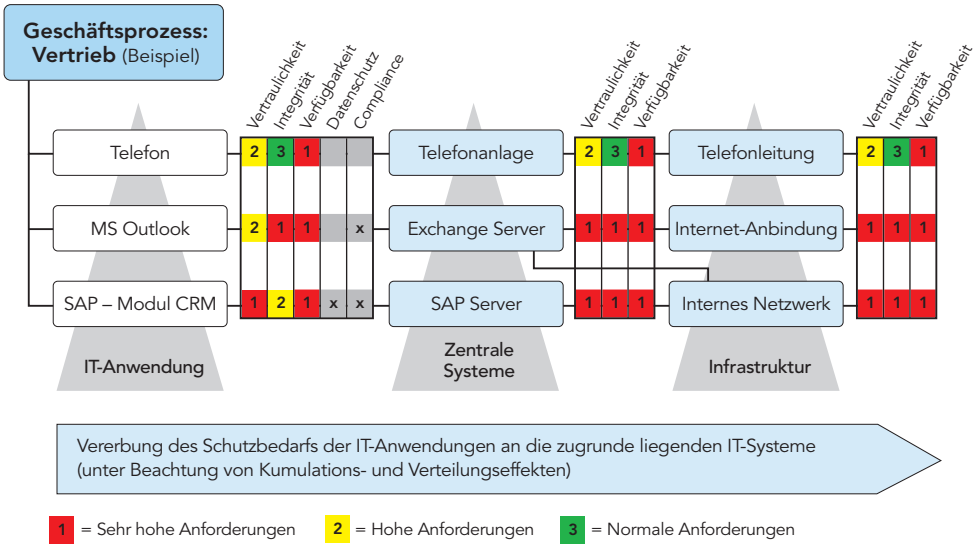
3. Je nach Priorität der unterstützten Geschäftsprozesse gilt es anschließend, den Schutzbedarf der IT-Anwendungen und -Systeme zu eruieren. Dies erfolgt, wie beschrieben, anhand der drei IT-Grundwerte „Vertraulichkeit, Integrität und Verfügbarkeit".

4. Unter Berücksichtigung der konzeptionellen und technischen IT-Sicherheitsanforderungen muss die IT-Umgebung dann einem umfassenden Audit unterzogen werden. Da Letzteres Fachwissen und Erfahrung voraussetzt und zudem eine neutrale Sichtweise gewährleistet sein muss, empfiehlt sich spätestens an dieser Stelle die Zusammenarbeit mit externen Spezialisten.

5. Sind die im Audit identifizierten und priorisierten Optimierungsmaßnahmen abgearbeitet, beginnt der beschriebene Prozess in einem regelmäßigen Abstand nach ein bis zwei Jahren von vorn. In den folgenden Prozesszyklen müssen bestehende Grundlagen wie die IT-Sicherheitsleitlinie oder die Organisationsstruktur dann an die sich ständig verändernden Anforderungen angepasst werden.

IT-Abhängigkeit von Geschäftsprozessen

Ausgehend von der Priorität des Geschäftsprozesses wird der Schutzbedarf der dazu benötigten IT-Anwendungen und -Systeme ermittelt.



Quelle: OneConsult Deutschland

Es gibt zahlreiche Standards, Rahmenwerke und technische Hilfsmittel, um den Prozess des IT-Sicherheits-Managements zu etablieren. Zu erwähnen sind allen voran die IT-Grundschutz-Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI), die detaillierte, wenn auch teilweise etwas theoretische Beschreibungen des Prozesses sowie konkreter IT-Sicherheitsmaßnahmen liefern. Für die praktische Umsetzung empfiehlt

Ohne Rückendeckung von oben ist angemessene Sicherheit nicht zu gewährleisten.

sich das Open-Source-Tool „Verinice“, das auf den Vorgaben der IT-Grundschutz-Standards aufsetzt. Darüber hinaus ist inzwischen auch der De-facto-Standard der Sparkassen-Finanzgruppe „Sicherer IT-Betrieb“ in einer Industrie- und Mittelstandsvariante erhältlich. Das Framework ist ebenfalls standardkonform und beschreibt eine auf Geschäftsprozessen basierende Vorgehensweise.

Fazit

Parallel zu den IT-Risiken wird auch die Abhängigkeit der Unternehmen von der IT weiter zunehmen. Ein den Anforderungen angemessenes Sicherheitsniveau ist ohne Rückendeckung des Managements nicht mehr zu gewährleisten – im ständigen Kampf um das IT-Budget werden notwendige IT-Sicherheitsmaßnahmen zwangsläufig auf der Strecke bleiben. Die Lösung liegt im proaktiven Handeln: Eine auf den Geschäftsprozessen basierende Betrachtung der IT-Themen reduziert deren Komplexität. Der IT-Verantwortliche schafft dadurch eine gemeinsame Kommunikationsbasis mit der Geschäftsführung. Im Dialog zwischen Geschäftsleitung, Fachabteilungen und IT-Abteilung lässt sich dann, ausgehend von den Anforderungen der Geschäftsprozesse an die IT, ein gemeinsames Verständnis für das erforderliche Sicherheitsniveau erarbeiten.

Die Kommunikation dieser Erkenntnisse in Form einer IT-Sicherheitsleitlinie sorgt für die dringend erforderliche Verankerung der IT-Sicherheit mit der Firmenstrategie. Der Stellenwert von IT und IT-Sicherheit im Unternehmen wird so auch in die Fachabteilungen transportiert. Das Spannungsfeld löst sich auf, und ein stabiles Fundament für das IT-Sicherheits-Management ist geschaffen. Auf diese Weise können die IT-Grundwerte nun strategie- und prozessgesteuert verteidigt werden. (kf) ◀

***Holger Gerlach** ist Geschäftsführer bei OneConsult Deutschland in Neu-Ulm.