Thema: IT-Basisschutz

Herausforderung IT-Grundschutz

Vorbei die Zeiten, in denen es genügte, die Firmen-IT mittels Firewall und Virenscanner zu schützen: Die heutigen Mindestanforderungen an die IT-Sicherheit umfassen mehr.

VON HOLGER GERLACH*

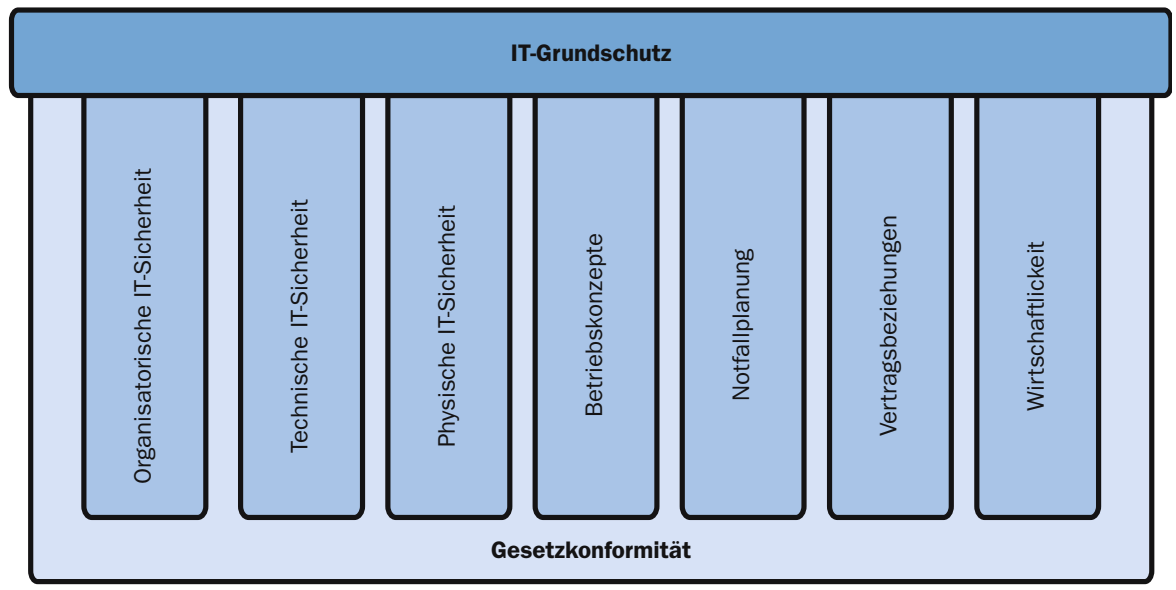
Der Begriff „IT-Grundschutz" bezeichnet die Etablierung technischer Sicherheitsmaßnahmen, die dem normalen Schutzbedarf angemessen sind. Was dem Begriff nach simpel klingt, ist in seiner Umsetzung komplex. Mit der Abhängigkeit der Unternehmen von der IT steigen auch die Anforderungen an die Sicherheit. Der IT-Grundschutz als Fundament für weitergehende Maßnahmen erfordert daher eine ganzheitliche Betrachtung.

Der Einsatz von Informationstechnologie im Unternehmen ist niemals Selbstzweck – direkt oder indirekt unterstützen IT-Anwendungen und -Systeme stets Geschäftsprozesse. Aus diesem Blickwinkel ist auch die IT-Sicherheit zu betrachten: Der Stellenwert der einzelnen Business-Abläufe und die Vertraulichkeit der verarbeiteten Daten geben das Niveau der zu treffenden Sicherheitsmaßnahmen vor.

Hier lesen Sie ...

- warum der IT-Grundschutz einen ganzheitlichen Ansatz erfordert;
- welche Faktoren dafür relevant sind;
- wie sich ein umfassender Basisschutz realisieren lässt;
- inwieweit das IT-GSHB dabei helfen kann.

Hinzu kommen externe Faktoren, die Unternehmen einen umfassenden IT-Grundschutz abverlangen: So sind Security-Audits von Kunden und Partnern insbesondere in der Zuliefererindustrie inzwischen übliche Praxis. Zudem sind Wirtschaftsprüfer und Datenschutzbeauftragte zu vertrauten Ansprechpartnern der IT-Abteilung geworden – hierbei diktieren nationale und internationale Vorschriften die Anforderungen an die technische Sicherheit. Darüber hinaus werden sich auch Banken und Versicherer künftig im Rahmen des Kunden-Ratings verstärkt dem Thema widmen. Ein weiterer wesentlicher Aspekt ist die zunehmende Kriminalität – von Angriffs- oder Betrugsversuchen einzelner Personen bis hin zur Wirtschaftsspionage.



Quelle: Gerlach

Diese Teilbereiche gilt es bei der Realisierung eines umfassenden IT-Grundschutzes zu beachten.

Beim Thema IT-Grundschutz sind im Wesentlichen acht Teilbereiche zu beachten. Eine Priorisierung dieser Bereiche ist im Sinne einer ganzheitlichen Betrachtung nicht sinnvoll, da jeder für sich essenzielle Bestandteile aufweist.

■ **Organisatorische IT-Sicherheit:** In diesen Bereich fällt primär der Aufbau des IT-Sicherheits-Managements. Dabei sollte die Geschäftsführung zunächst eine IT-Sicherheitsleitlinie formulieren, die strategische Aussagen zum Thema enthält. Zudem müssen eindeutige Verantwortlichkeiten inklusive Vertretungsregelungen sowie Kommunikationswege definiert werden. Zu den weiteren Aufgaben zählt, alle Maßnahmen und Veränderungen zu dokumentieren, die IT-Benutzer zu schulen, für Sicherheit zu sensibilisieren sowie regelmäßige Audits etwa in Form von Penetrationstests vorzunehmen. An dieser Stelle entscheidet sich, ob IT-Sicherheit vom Management, den Administratoren und den IT-Benutzern als Prozess verstanden und gelebt wird.

■ **Technische IT-Sicherheit:** Firewall, Virenscanner und Verschlüsselungssysteme sind wohl die gängigsten Beispiele für IT-Sicherheitsvorkehrungen. Darüber hinaus sollte jedoch ein schlüssiges und umfassendes Rollen- und Rechtekonzept implementiert und dokumentiert sein. Auch Maßnahmen wie Patch-Level-Management und Systemhärtung sowie die Absicherung drahtloser Kommunikationswege (etwa WLAN) fallen in diesen Bereich. Es empfiehlt sich zudem, die wesentlichen IT-Strukturen – insbesondere die Übergänge zu Fremdnetzen – in einem Netzplan zu dokumentieren.

■ **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-Grundschutz 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 Störfällen voraus. Ebenfalls zu berücksichtigen sind das System- und Netz-Management sowie die Steuerung von Systemkapazitäten und -verfügbarkeiten. Dieser Bereich ist umso wichtiger, je größer die IT-Umgebung ist.

■ **Notfallplanung:** Umfassende 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, müssen die Notfallpläne dort zwingend integriert werden.

■ **Vertragsbeziehungen:** Verträge mit externen Dienstleistern müssen Verfügbarkeiten, Reaktions- und Behebungszeiten sowie die Verschwiegenheit der einzelnen Mitarbeiter verbindlich gewährleisten. Auch gesetzliche Aspekte wie die Anforderungen des Bundesdatenschutzgesetzes (BDSG) sind vertraglich abzudecken. Vor allem beim Outsourcing von IT-Systemen sollte sich der Auftraggeber das Recht auf die Auditierung seines Partners einräumen lassen.

■ **Wirtschaftlichkeit:** Neben der Wirksamkeit der Sicherheitsmaßnahmen muss die IT-Abteilung auch nachweisen, dass diese angemessen sind. So gilt es, Aufwendungen für sicherheitsspezifische Technik, Softwarelizenzen oder Personal gegenüber der Geschäftsführung und den Fachabteilungen transparent zu machen. Existiert eine Kostenstellenrechnung, 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

IT-Grundschutz bei der Sparkassen-Finanzgruppe

Die **Sparkassen-Finanzgruppe** gilt derzeit mit etwa 650 Unternehmen als der weltweit größte Verbund von Finanzdienstleistern. Annähernd 400 000 Mitarbeiter arbeiten mit IT-Systemen wie PC oder Notebook. Die Zusammenarbeit im Verbund bedingt eine weitreichende Vernetzung der IT. Die Realisierung eines **verbundübergreifenden IT-Sicherheitsniveaus** ist dadurch obligatorisch. Um einen **einheitlichen Mindestschutz** zu gewährleisten, hat das SIZ (Informatikzentrum der Sparkassenorganisation) mit dem Produkt „Sicherer IT-Betrieb" einen **De-facto-Standard** geschaffen. Dieser deckt die Vorgaben aller gängigen IT-Sicherheitsstandards wie IT-GSHB, ISO/IEC 17799 und ISO 27001 ab und erfüllt zudem die relevanten Anforderungen von externen Stellen wie Wirtschaftsprüfern, Gesetzgebern und Aufsichtsbehörden.

Um den Unternehmen der Sparkassen-Finanzgruppe die Umsetzung eines **fundierten und umfassenden IT-Grundschutzes** zu erleichtern, haben die Spezialisten des SIZ zahlreiche Konzepte und Dokumentenvorlagen erarbeitet. Bemerkenswert ist insbesondere ein Fragenkatalog für einen **strukturierten Soll-Ist-Vergleich,** der mehr als 150 Hauptfragen und ein Mehrfaches an vertiefenden Unterfragen umfasst. Der Fragenkatalog spiegelt die genannten Standardvorgaben und externen Anforderungen wider. Vorteile ergeben sich für die Verbundunternehmen aus der **Vereinheitlichung der Mindestanforderungen,** der Verbesserung des Projektverlaufs und vor allem aus der zuverlässigen Bestimmbarkeit des zu erwartenden Aufwands. Fehlt es an Letzterem, scheitern entsprechende Projekte in Unternehmen aus Industrie und Mittelstand häufig.

von Jahr zu Jahr länger. Trotz unterschiedlicher Formulierung bleibt eine Anforderung gleich: Die Pflicht, für einen fundierten IT-Grundschutz 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).

In den hier beschriebenen Teilbereichen sind jeweils nur wesentliche Beispiele für sinnvolle IT-Sicherheitsmaßnahmen aufgeführt. Die derzeit detaillierteste Darstellung von Methoden, Prozessen und Maßnahmen im Hinblick auf IT-Security bietet das IT-Grundschutz-Handbuch (IT-GSHB) des Bundesamts für Sicherheit in der Informationstechnik (BSI). Hilfreich sind die themenspezifisch geordneten Ausführungen sowohl zur Implementierung von Maßnahmen als auch zur regelmäßigen Erfolgskontrolle. Infolge seiner Umstrukturierung ist das aktuelle IT-GSHB nun vollständig kompatibel zu der 2005 verabschiedeten internationalen Norm „ISO/IEC 27001:2005“.

Mehr zum Thema

www.computerwoche.de/

1207801: BSI erweitert Schutzhandbuch;
568258: Security: Nur so viel wie notwendig;
1051633: IT-Sicherheit ist Chefsache.

www.computerwoche.de/security-expertenrat

Projektverlauf nach IT-GSHB

Basis eines fundierten IT-Grundschutzes ist das IT-Sicherheits-Management: Hier wird der Prozess bezüglich Planung, Umsetzung, Kontrolle und Optimierung (PDCA-Modell) geschaffen. Daher empfiehlt es sich, vor allem den Bereich „100-2“ des BSI-Standards, sprich: die IT-Grundschutz-Vorgehensweise, zu berücksichtigen. Darauf basierende Projekte umfassen im Wesentlichen folgende Phasen: Zunächst müssen Unternehmen eine IT-Sicherheitsleitlinie formulieren, die strategische Aussagen der Geschäftsführung zum Thema enthält. Daraufhin gilt es, eine der Firmengröße angemessene Organisationsstruktur zu etablieren. Eines der Hauptziele dieser Projektphase ist es, die jeweiligen Verantwortlichkeiten klar zu definieren.

Die dokumentarische Grundlage des Projekts ist die so genannte Strukturanalyse. Sie erfordert – neben einem möglichst übersichtlichen Netzplan – die Erfassung aller IT-Anwendungen und -Systeme sowie Netzkomponenten. Detailliertes Wissen über Gesamtumfang und Ausprägung der IT-Umgebung ist eine Grundvoraussetzung, um Sicherheitsschwachstellen erkennen zu können. Die Praxis zeigt jedoch, dass diese Informationen häufig weder zentral noch geordnet vorliegen.

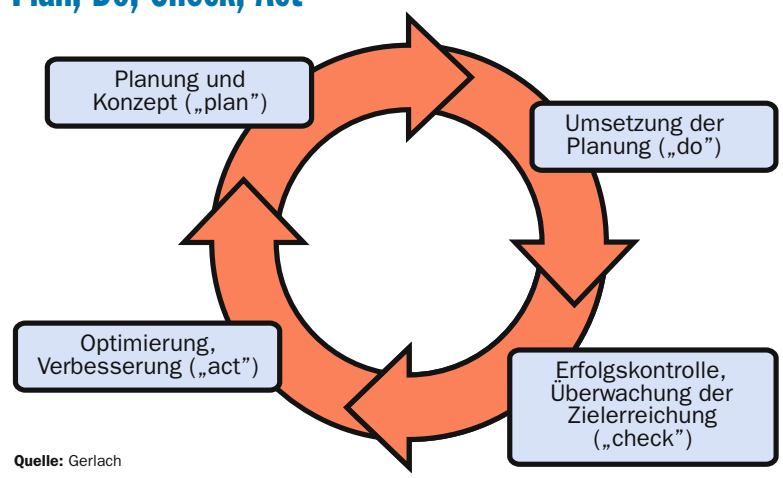
Anschließend gilt es, je nach Wichtigkeit der unterstützten Geschäftsprozesse den Schutzbedarf der Anwendungen und Systeme zu ermitteln. Dies erfolgt anhand der drei IT-Grundwerte „Vertraulichkeit“, „Integrität“ und „Verfügbarkeit“.

Der anschließende Soll-Ist-Vergleich stellt angesichts der Vielschichtigkeit des IT-Grundschutzes eine der größten Herausforderungen innerhalb des Projekts dar. Hierzu ist die IT-Umgebung unter Berücksichtigung des jeweiligen Schutzbedarfs einem umfassenden Audit zu unterziehen, was auf Basis der IT-GSHB-Vorgaben erfolgen kann. Da eine solche Überprüfung Fachwissen und Erfahrung voraussetzt, empfiehlt es sich, in dieser Projektphase mit externen Spezialisten zusammenzuarbeiten. Sie verfügen im Idealfall über standardkonforme Check-Listen, um den Audit-Verlauf zu verbessern und zu beschleunigen. Nach der Abarbeitung der identifizierten Verbesserungsmaßnahmen muss der beschriebene Prozess in regelmäßigen Intervallen wiederholt werden. In den darauf folgenden Projektzyklen werden dann die bestehenden Grundlagen, beispielsweise die IT-Sicherheitsleitlinie oder die Organisationsstruktur, den sich ständig wandelnden Anforderungen angepasst.

Basis IT-Sicherheits-Management

IT-Sicherheit hat sich demnach zu einer komplexen Spezialdisziplin innerhalb des Unternehmens entwickelt und muss von den Verantwortlichen auch entsprechend gelebt werden. In akuten Sicherheitsvorfällen begründeter Aktionismus oder Insellösungen sind weder zielführend noch wirtschaftlich. Das Fundament eines umfassenden IT-Grundschutzes liegt im IT-Sicherheits-Management. Dort werden die Weichen für eine effiziente und stabile IT gestellt und damit wesentliche Grundlagen für den Unternehmenserfolg gesichert. *(kf)* ◆

Plan, Do, Check, Act



Quelle: Gerlach

Anhand des PDCA-Modells (Plan, Do, Check, Act) lässt sich der IT-Grundschutz aufrechterhalten und kontinuierlich verbessern.

*__HOLGER GERLACH__ ist lizenzierter IT-Grundschutz-Auditor in Neu-Ulm.