

# Frischzellenkur für IT-Grundschutz-Kataloge

## Neues in der 11. Ergänzungslieferung der IT-Grundschutz-Kataloge

Elmar Török, bits+bites

**Die 11. Ergänzungslieferung der IT-Grundschutz-Kataloge des BSI steht an. Im Infodienst IT-Grundschutz finden Sie bereits heute eine Zusammenfassung der neuen und überarbeiteten Themen.**

Anforderungen und Aufgaben der IT-Sicherheit ändern sich, die IT-Grundschutz-Kataloge werden diesem Wechsel durch regelmäßige Ergänzungslieferungen gerecht. Jährliche Bedarfsabfragen bei den registrierten Anwendern helfen dem BSI, die wichtigen Themen zu finden, die den Anwendern aktuell unter den Nägeln brennen. Die nächste Ergänzungslieferung, die 11. in der Geschichte der IT-Grundschutz-Kataloge, befasst sich mit den folgenden Themen:

### Löschen und Vernichten von Daten

Auf ausgesonderten, weitergegebenen oder gebraucht gekauften Datenträgern finden sich häufig noch vertrauliche Informationen, obwohl diese die Institution nicht hätten verlassen dürfen. Der Baustein B 1.15 „Löschen und Vernichten von Daten“ beschreibt, welche Verfahren und Methoden geeignet sind, um Daten bzw. Datenträger vollständig und zuverlässig zu löschen oder Datenträger zu vernichten. Jede Institution sollte eine geregelte Vorgehensweise für die Löschung oder Vernichtung von Datenträgern haben, um den Missbrauch der gespeicherten Informationen zu verhindern. Darin müssen sowohl digitale Datenträger wie Festplatten als auch analoge Datenträger wie Papierenbezogen werden.

### Anforderungsmanagement

Jede Institution muss alle für sie und ihre Geschäftsprozesse relevanten gesetzlichen, vertraglichen und sonstigen Vorgaben identifizieren und deren Einhaltung durch angemessene Überwachungsmaßnahmen sicherstellen. Diese Aufgabe ist durch einige neue Gesetze stärker in den Fokus gerückt und wird häufig unter dem Stichwort Compliance diskutiert. Der Baustein B 1.16 „Anforderungsmanagement“ enthält keine wesentlichen neuen Maßnahmen. Zur besseren Vergleichbarkeit mit den Normen ISO 27001 und 27002 wurden hier Maßnahmen zusammengestellt, die die Controls zum Thema „Compliance“ abdecken.

### Schutz vor Schadprogrammen

Der Baustein B 1.6 beschäftigte sich bisher unter dem Titel „Computer-Viren-Schutzkonzept“ damit, geeignete Maßnahmen zum Schutz vor Schadprogrammen zu empfehlen. Die Palette der Schadprogramme ist allerdings deutlich größer geworden. Neben Computer-Viren müssen auch Trojanische Pferde, Computer-Würmer und weitere Arten von Schaden verursachender Software abgewehrt werden. Daher wurde der Baustein nicht nur grundlegend überarbeitet, sondern auch in B 1.6 „Schutz vor Schadprogrammen“ umbenannt.

### Überarbeitung Notfallmanagement

Im Dezember 2008 wurde der BSI-Standard 100-4 „Notfallmanagement“ veröffentlicht. Bereits während dessen Erstellung wurde begonnen, den Baustein B 1.3 „Notfallmanagement“ zu überarbeiten. Der Baustein baut auf dem BSI-Standard 100-4 auf und fasst dessen wichtigste Aspekte zum Notfallmanagement zusammen. Im Baustein wird aufgezeigt, wie ein funktionierendes Notfallmanagement in einer Behörde oder einem Unternehmen eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu die wesentlichen Schritte in einem systematischen Notfallmanagement-Prozess und gibt Anleitungen zur Erstellung eines umfassenden Notfallkonzeptes.

### Überarbeitung Behandlung von Sicherheitsvorfällen

Der Baustein B 1.8 „Behandlung von Sicherheitsvorfällen“ konzentriert sich auf IT-Sicherheitsvorfälle. Um auch bei akuten Sicherheitsproblemen wie Schadsoftware-Infektionen die IT sicher betreiben und Schäden eindämmen zu können, müssen im Vorfeld Verfahren geplant, aufgesetzt und eingeübt werden (Security Incident Handling oder auch Security Incident Response). Ausführlich betrachtet wird in diesen Baustein unter anderem der Aspekt Computer-Forensik, also welche Maßnahmen zur Beweissicherung bei Sicherheitsvorfällen ergriffen werden sollten.

### Samba

Im Baustein B 5.17 „Samba“ werden die grundsätzlichen Sicherheitseigenschaften von Samba betrachtet. Samba ist ein frei verfügbarer Authentisierungs-, Datei- und Druckdienst und ermöglicht

Interoperabilität zwischen Betriebssystemen auf Basis von Microsoft Windows und der Unix-Welt.

## Windows Vista

Der Baustein B 3.210 „Client unter Windows Vista“ ergänzt die Reihe von Bausteinen, die sich mit dem sicheren Einsatz von Windows-Betriebssystemen beschäftigen. Der vorliegende Baustein behandelt das Client-Betriebssystem Windows Vista in der Version Enterprise, kurz Windows Vista Enterprise. Hier wird der Anwender auf konzeptionelle Sicherheitsaspekte, aber auch auf Sicherheitsempfehlungen zu konkreten Konfigurationseinstellungen hingewiesen.

## Peer-to-Peer-Dienste

Der bisherige Baustein B 5.1 „Peer-to-Peer-Dienste“ wird mit der 11. Ergänzungslieferung entfernt. Er befasste sich ausschließlich mit Clients, die sich Ressourcen in einem lokalen Netz gegenseitig zur Verfügung stellen und fokussierte hauptsächlich auf Windows-Clients. Mittlerweile wird der Begriff „Peer-to-Peer“ meist für den Austausch von Informationen im Internet verwendet. Neben Dateien, die mit bekannten und unbekanntenen Personen geteilt werden können, kann unter Verwendung von Peer-to-Peer-Diensten beispielsweise auch über das Internet telefoniert werden. Diese Aspekte werden nun in der Maßnahme M 5.152 „Austausch von Informationen und Ressourcen über Peer-to-Peer-Dienste“ zusammengefasst betrachtet. Die Maßnahme wurde in den Baustein B 3.201 „Allgemeiner Client“ integriert.

## Überarbeitung Rechenzentrum

Der Baustein B 2.9 „Rechenzentrum“ wurde an aktuelle Standards und Entwicklungen angepasst. Ein Rechenzentrum stellt eine wichti-

ge zentrale Einheit mit besonderen Sicherheitsanforderungen dar, beispielsweise beim Brandschutz, der Energieversorgung und der Zutrittskontrolle. Bei der Überarbeitung wurden neue Erkenntnisse im Bereich der Energieversorgung ausgeführt. Außerdem wurde der Baustein um Maßnahmen wie die Durchführung von Funktionstests der technischen Infrastruktur ergänzt, mit denen beispielsweise die ordnungsgemäße Funktion der Notenergieversorgung oder das korrekte Zusammenspiel von Klimatisierung und Brandschutz getestet werden sollten.

## Neue Maßnahmen und Gefährdungen

Außerdem sind verschiedene neue Maßnahmen und Gefährdungen aufgenommen worden, beispielsweise zu den Themen Data Leakage Prevention (M 4.345 Schutz vor unerwünschten Informationsabflüssen) und M 6.137 Treuhänderische Hinterlegung (Escrow). Neben verschiedenen Bausteinen, die der 11. Ergänzungslieferung hinzugefügt wurden, wurden auch Bausteine entfernt, und zwar die „NT-Bausteine“, da hier Betriebssysteme betrachtet wurden, die sich mittlerweile kaum noch in Institutionen im Einsatz befinden. Für die Anwender, die diese Betriebssysteme noch im Einsatz haben, werden die Bausteine weiterhin unter den Hilfsmitteln zum IT-Grundschutz zur Verfügung stehen.

## Prüffragen

Bisher wurden am Ende vieler Maßnahmen ergänzende Kontrollfragen angeführt, die das behandelte Thema abrunden und nochmals einen kritischen Blick auf die Umsetzung der Maßnahmen bewirken sollten. Diese ergänzenden Kontrollfragen sollten Denkanstöße geben, aber keine Prüffragen ersetzen. Sie können also beispiels-

weise nicht bei Revisionen oder Audits eingesetzt werden, um den Umsetzungsgrad einer Maßnahme zu bestimmen. Sie erhoben auch nie einen Anspruch auf Vollständigkeit. Da dies immer wieder zu Verwirrungen führte, werden die ergänzenden Kontrollfragen in neuen Bausteinen durch Prüffragen abgelöst. Diese sind so formuliert, dass sie als letzte Checkliste benutzt werden können, um die Umsetzung der Maßnahmen kontrollieren zu können. Sie geben Ziel und Grundrichtung der Sicherheitsempfehlungen vor und können damit als Grundlage für Revisionen und Zertifizierungsaudits benutzt werden.

## Aktualisierung und Überarbeitung

Da der Begriff „Informationssicherheit“ umfassender ist als der Ausdruck „IT-Sicherheit“, wird zunehmend ersterer verwendet. IT-Grundschutz verfolgt schon lange einen ganzheitlichen Ansatz, bei dem auch geschäftsrelevante Informationen und Geschäftsprozesse geschützt werden sollen, die nicht oder nur teilweise durch IT unterstützt werden. Der Begriff „IT-Sicherheit“ ist eingeführt und weit verbreitet, daher wird er in dieser sowie in anderen Publikationen des IT-Grundschutzes weiterhin häufig verwendet, allerdings werden die Texte sukzessive stärker auf die Betrachtung von Informationssicherheit ausgerichtet. Weitere strukturelle Veränderungen wurden in der aktualisierten Ausgabe nicht durchgeführt. Die Nummerierung bestehender Gefährdungen und Maßnahmen blieb erhalten, sodass ein im Vorjahr auf Basis der IT-Grundschutz-Kataloge erstelltes Sicherheitskonzept fortgeschrieben werden kann.