Der Grundschutzkatalog: Sicherheit nach Plan

Computersicherheit ist extrem komplex: IT-Grundschutzkataloge helfen, den Überblick zu behalten. Sie haben sich seit zehn Jahren bewährt. VON HARTMUT GOEBEL

Die wichtigsten Bausteine des BSI-Grundschutzkatalogs (www.bsi.de)

QUELLE: OLIVER NIESS, WIKIPEDIA.ORG

HIER LESEN SIE...

- Kleine Fehler mit schlimmen Folgen: Warum ein Security-System wichtig ist
- Auf welchen Stufen der Grundschutz basiert
- Welche Tools Sie dafür brauchen

Wegen eines Plattendefekts ist der Fileserver ausgefallen. Seit zwei Tagen können die fünf Mitarbeiter des Ingenieurbüros Behmer nicht richtig arbeiten. Zu allem Unglück ist Ingenieur Meder im Urlaub, der sich sonst um die EDV kümmert. Morgen sollen endlich die neuen Platten kommen, dann dauert es noch einmal einen halben Tag, um das Backup zurück zu spielen. Am nächsten Tag grosse Aufregung: Teile des Backups sind nicht lesbar. Zwar gibt es von den wichtigsten Konstruktionsplänen Ausdrucke, aber es wird Monate dauern, alle Zeichnungen neu zu erstellen. Unglaublich? Leider viel zu oft Realität.

Hartmut Goebel, Inhaber von Goebel Consult (www.goebel-consult.de), ist spezialisiert auf IT-Sicherheit, Security Audits und die IT-Grundschutzkataloge

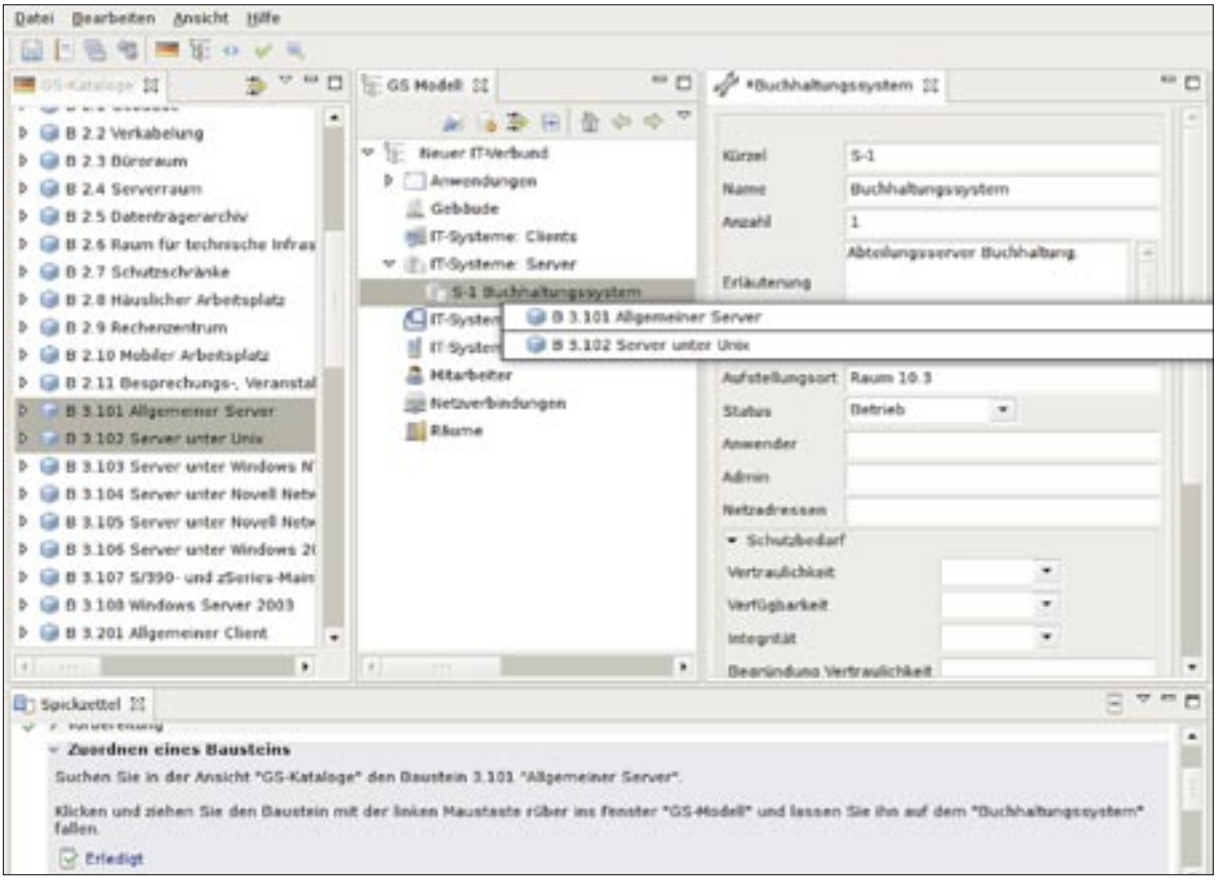
Der Administrator der Schmidt AG hat im letzten Monat gekündigt. Sein Nachfolger wird seit vier Wochen eingearbeitet. Auch im Vertrieb hat es eine Veränderung gegeben: Für Herrn Angerer ist nun Frau Rader im Unternehmen. Frau Rader wartet seit zwei Wochen darauf, einen Remote-Zugang zum Firmennetz zu bekommen. Herr Angerer hat seinen noch immer. Der neue Administrator hat so viel Arbeit, dass er nicht dazukommt, den einen einzurichten und den anderen zu sperren. Vorher muss er noch herausfinden, wie die Zugänge administriert werden, denn Dokumentation gibt es nicht. Unglaublich? Leider nur ein Beispiel unter vielen.

Was ist hier schief gelaufen? Eigentlich nur Kleinigkeiten: Dem Ingenieurbüro Behmer fehlt ein RAID-System. Zudem hatte niemand geprüft, ob man das Backup zurückspielen kann. Bei der Schmidt AG wurden zwei wichtige Prozesse nicht dokumentiert: Was ist zu tun, wenn ein Mitarbeiter ausscheidet, und wie richtet man einen Remote-Zugang für neue Mitarbeiter ein. Um allgemeine Fehler wie diese zu vermeiden, wären Richtlinien nützlich, an denen sich das Unternehmen orientieren kann. Damit wären 80 Prozent der gängigsten Sicherheitsprobleme beseitigt. Die Verantwortlichen hätten den Kopf frei für die restlichen 20 Prozent und vor allem für das eigentliche Business. Um im Bild zu bleiben: Das Ingenieurbüro Behmer verdient nichts mit dem Fileserver. Fällt der Rechner aber aus, entstehen unter Umständen hohe Kosten.

Richtlinien für sichere IT-Systeme

Die IT-Grundschutzkataloge des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) geben solche allgemein gültigen Richtlinien an die Hand (www.bsi.de). Zu den Katalogen gehört auch eine konkrete Handlungsanweisung:

- Zunächst sind alle Computersysteme und Anwendungen in Gruppen einzuteilen: Windows-PCs, Rechner für die Buchhaltung, die Datenbank, der Webserver, das ERP-System, die Personalabteilung. Selbstredend kann ein System zu mehreren Gruppen gehören. Zum Beispiel ist der Webserver gleichzeitig ein Linux-Server, die Rechner in der Personalabteilung auch Windows-PCs.
- Für jede Gruppe muss definiert werden, ob die grundlegende Sicherheit (Baseline) ausreichend ist, oder ob höhere Anforderungen gelten. Da in der Personalabteilung



Die Open-Source-Software Verinice (www.verinice.org) ist kostenlos und unterstützt Unternehmen bei der Umsetzung des Grundschutzkatalogs

personenbezogene Daten verarbeitet werden, muss hier der Datenschutz besonders berücksichtigt werden. Das ERP-System darf zum Beispiel nicht länger als zwei Stunden ausfallen, weil die Mitarbeiter sonst das Tagesgeschäft nicht erledigen können.

- Im Bausteinkatalog der IT-Grundschutzkataloge wird nun für jede Gruppen ermittelt, welche Gefährdungen bestehen und welche Massnahmen vorgeschlagen werden. Die Gefährdungen sind jeweils aufgeteilt in höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen und vorsätzliche Handlungen. Zum Beispiel: Für ein Rechnerzentrum gibt es die Gefährdung «Unbefugter Zutritt zu schutzbedürftigen Räumen». Dieses Problem zählt zu den organisatorischen Mängeln, da es sich mit Vorschriften beseitigen lässt.
- Zu den Massnahmen ist jeweils aufgeführt, wie wichtig sie sind – Prioritäten A bis C sowie Z für zusätzlich oder optional – und wer verantwortlich ist. Bei einem allgemeinen Server hat die Massnahme «Hinterlegen des Passwortes» die Priorität A, das «Einrichten einer Testumgebung für einen Server» ist aber nur Priorität Z. Anhand dieser Einordnung legen Unternehmen fest, welche Massnahmen zuerst umgesetzt werden müssen.

In der Onlineversion der IT-Grundschutzkataloge (www.bsi.de/gshb) sind Gefährdungen und Massnahmen abrufbar. Per Mausklick ermitteln Sie hier, welche Gefahr bei der «Nutzung des RAS-Clients als RAS-Server» besteht oder was bei «Notfallvorsorge für einen Server» zu tun ist.

Das Ingenieurbüro Behmer hätte nun eine schöne Liste: erstens ein RAID-System einrichten, zweitens den Händler zur schnellen Lieferung verpflichten und drittens regelmässig Prüfen, ob sich die Backups zurückspielen lassen. Was davon gemacht wird, entscheidet natürlich Herr Behmer, der Chef. Wie ist jedoch die Urlaubsvertretung für Herrn Meder geregelt? Dafür gibt es einen eigenen Baustein «Übergeordnete Aspekte». Dort finden sich unter «Personal» die «Vertretungsregelungen».

Ressourcen und Tools

Auf den ersten Blick klingt das nach viel Aufwand. Ein erfahrener Berater benötigt für eine Bestandsaufnahme jedoch nur zwei bis drei Tage. Dann kann er abschätzen, wie gut oder weniger gut es um die IT-Security der Firma bestellt ist. Allerdings ist der externe Berater gar nicht unbedingt erforderlich: Die IT-Grundschutzkataloge sind ausführlich genug, um von einem Sicherheitsbeauftragten selbstständig abgearbeitet zu werden. Jedoch hat ein externer Berater immer einen anderen Blickwinkel und kann unbefangener an die Untersuchung herangehen.

Das Anwenden der IT-Grundschutzkataloge unterstützt ausserdem ein Tool: Verinice (http://verinice.org) ist Open Source und in Java implementiert, also auf allen wichtigen Plattformen einsetzbar. Das Tool hilft, die Systeme zu erfassen, zu gruppieren und Massnahmen mit den verantwortlichen Personen festzulegen. Auch kann – als Fortschrittskontrolle – dokumentiert werden, welche Massnahmen umgesetzt wurden.

Mit den IT-Grundschutzkatalogen lässt sich ein Grossteil der Risiken von Computeranlagen in den Griff bekommen. Sowohl die Kataloge also auch das Tool Verinice sind kostenlos. IT-Sicherheit kann also einfach und kostengünstig sein. Fazit: Es gibt keine Ausreden mehr, sich nicht um eine vernünftige Security-Strategie zu kümmern. ■

IT-GRUNDSCHUTZKATALOGE

Die wichtigsten Bausteine

- Allgemeines: beschreibt Idee und Vorgehensweise
- Bausteinkatalog: unterteilt die Komponenten in übergreifende Aspekte, Infrastruktur, IT-Systeme, Netze und IT-Anwendungen
- Gefährdungskatalog: enthält die Gefährdungen, zum Beispiel Brand, Ausspähen von Daten, Hardware-Ausfall
- Massnahmenkatalog: enthält Gegenmassnahmen etwa Brandschutz, Verschlüsselung und Ersatzgeräte
- Rollendefinition: Wer ist wofür zuständig?