Der IT-Grundschutz setzt bei der IT-Organisation an. Ausgangspunkt ist die übliche Gefährdung der betrachteten Systeme – also etwas, was für gut 80 % der Fälle zutrifft und als Schutz ausreicht. Bild: Fotolia

Modernisiertes Kompendium erleichtert Mittelständlern den Einstieg

Neuerungen *näher an der* Praxis

IT-Grundschutz | Das in die Jahre gekommene Kompendium hat sich aufgebläht. An einer schlanken Neuauflage arbeitet derzeit das Bundesamt für Sicherheit in der Informationstechnik (BSI). 2016 sollen konkretere Konzepte veröffentlicht werden.

80 Bausteine, 1260 Einzelmaßnahmen, 4500 Seiten – so wuchtig ist der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI). 1993 als schmale Sammlung von Best Practices für Behörden ins Leben gerufen, ist das Kompendium inzwischen kaum noch zu überblicken. Vor allem Mittelständler sind mit der Umsetzung oft überfordert. Die Liste der Kritikpunkte ist lang: Zu viele Rollen mit strikter Trennung, ausufernde Dokumentationspflichten, hoher Aufwand ohne Abwägung der Wirtschaftlichkeit und zu träge Erweiterung auf neue technologische Entwicklungen.

Doch trotz aller Kritik ist das BSI-Konzept „IT-Grundschutz" eine Erfolgsgeschichte. Wie viele Unternehmen wirklich den IT-Grundschutz einsetzen, ist für Holger Schildt vom BSI schwer einzuschätzen. Genaue Zahlen gibt es nicht. „Unsere Veranstaltungen sind binnen kurzer Frist immer ausgebucht", nennt er als Anhaltspunkt. „Ich sehe nach wie vor eine hohe Nachfrage nach dem IT-Grundschutz".

Vor allem mittelgroße Unternehmen profitieren vom Grundschutz-Konzept, sie können sich damit den hohen Aufwand der ISO 27 000 ersparen. Bei den ISO-Normen geht es in erster Linie um die Verankerung eines Managementsystems zur Informationssicherheit in allen Bereichen eines Unternehmens. Der IT-Grundschutz dagegen setzt direkt bei der IT-Organisation an. Ausgangspunkt ist die übliche Gefährdung der betrachteten Systeme – also etwas, was für gut 80 % der Fälle zutrifft und als Schutz ausreicht. Wer einen höheren Schutzbedarf hat, benötigt ohnehin eine individuelle Lösung.

Vor allem aus Sicht eines Mittelständlers hat der IT-Grundschutz deshalb drei Vorteile gegenüber den ISO-Normen: Erstens setzt er ganz pragmatisch an den IT-Systemen an. Zweitens ist er sehr konkret und bietet viele praktische Hinweise für die Umsetzung. Drittens verzichtet er weitgehend auf aufwendige Risikoanalysen.

Neue Technologien bringen neue Gefahren

Was vor zehn Jahren Sicherheitsstandard war, bietet heute höchstens halbe Sicherheit. „Wir haben Elemente wie Virtualisierung und Cloud Computing eingebaut", sagt Holger Schildt. Doch angesichts der technologischen Dynamik haben sich die eigentlichen Vorteile des IT-Grundschutzes beinahe ins Gegenteil verkehrt. „Die Einstiegshürde für die Umsetzung des jetzigen IT-Grundschutzes ist oft sehr hoch."

Der Umsetzungsaufwand ist im Laufe der Jahre erheblich gestiegen und auch das Sicherheitsniveau ist für viele Anwendungsfälle zu hoch. Es heißt IT-Grundschutz, aber viele Empfehlungen der Bausteine liegen weit jenseits einer Basissicherheit. Deshalb arbeitet das BSI schon länger an einer Grundrenovierung seiner Kataloge und Vorgehensweisen. 2016 sollen konkretere Konzepte veröffentlicht und weiterhin Feedback von den Anwendern eingeholt werden.

Holger Schildt vom BSI sieht „nach wie vor eine hohe Nachfrage nach dem IT-Grundschutz" aufgrund stets ausgebuchter Veranstaltungen.

Sofortmaßnahmen und Kronjuwelen

Der neue IT-Grundschutz teilt die Maßnahmen zunächst in drei aufeinander aufbauende Ebenen ein, die eine Skalierung der Absicherung bewirken. So soll die Größe des Projektes überschaubarer werden und den Einstieg erleichtern – bisher schreckt diese viele kleinere Unternehmen, aber auch gestandene Mittelständler eher ab.

Auf der ersten Ebene stehen Sofortmaßnahmen. Sie sollten insbesondere bei kleineren Unternehmen vorrangig für eine schnelle Absicherung der eigenen IT-Infrastruktur umgesetzt werden. Oft sind solche Basisempfehlungen ohne großen analytischen Ballast selbstverständlich und rasch umzusetzen – etwa regelmäßige Datensicherungen oder Virenschutz. Die zweite Ebene bilden Standardempfehlungen für den normalen Schutzbedarf, die für den Großteil der Unternehmen auch ohne präzise Risikoanalyse möglich sind. Auf der dritten Ebene finden sich dann Hochsicherheitsmaßnahmen. Sie widmen sich Organisationen mit einem erhöhten Schutzbedarf.

Auch auf der Seite der Methodik soll der neue IT-Grundschutz größere Flexibilität bringen. So plant das BSI einerseits eine Art „Instantmethodik", bei der die Maßnahmen ohne Feststellung des Schutzbedarfs und ohne Risikoanalysen ganz pragmatisch nach Bedarf eingeführt werden, angefangen bei den relevanten Basisempfehlungen. Neu eingeführt wird die sogenannte Kronjuwelen-Methode. Hierbei findet der IT-Grundschutz auf einen sehr kleinen Teil der Institution Anwendung, auf jenen mit den zuvor in einer Analyse identifizierten essentiellen Assets. Voraussichtlich wird sich die Vorgehensweise „Kernabsicherung" nennen. Auch bei dieser Methodik geht es in erster Linie um eine pragmatische Vorgehensweise, die schnelle Ergebnisse bei geringem Aufwand verspricht. Außerdem präsentiert das BSI als dritte Methode den traditionellen Planungsansatz, der mit einer umfangreichen Schutzbedarfsermittlung beginnt und dann zu den Maßnahmen überleitet. Kurz: Der neue Grundschutz wird stärker auf die Bedürfnisse von real existierenden Unternehmen eingehen, die mit ihren Mitteln auch bei der IT-Sicherheit haushalten müssen und von einer niedrigeren Einstiegsschwelle des IT-Grundschutzes profitieren.

„Mittelständler haben erhöhten Bedarf bei Schwachstellenscans und beim Notfallmanagement", weiß Lutz Kolmey von Mod IT Services.

Alle Bausteine auf zehn Seiten

Eine große Neuerung wird die entschlackte Darstellung des IT-Grundschutzes sein. Hier soll es einen deutlichen Bruch mit der bisherigen Praxis geben. Die Dokumente gliedern sich zwar wie bisher in thematische Bausteine. Sie sind jedoch nach Zielgruppen in zwei Teile aufgeteilt. Die Bausteine richten sich vorrangig an den IT-Sicherheitsverantwortlichen und nennen die Anforderungen. Diese Anforderungen sollten im Detail in der Regel von Administratoren und IT-Fachleuten umgesetzt werden. Dabei gibt es Verweise auf Dokumente, wie diese Anforderungen umgesetzt werden können.

So gibt es etwa zehn Seiten, die die Bausteine und ihre Anforderungen umfassen und sich an den Sicherheitsverantwortlichen richten. Hier wird beschrieben, welche Maßnahmen umgesetzt werden müssen – die Leitfrage lautet, „Was muss gemacht werden?" Für die Hauptzielgruppe der IT-Mitarbeiter veröffentlicht das BSI zusätzliche Hinweise, wie die Anforderungen der Bausteine umgesetzt werden können. Sie enthalten detailreiche und vertiefende Empfehlungen zu den Maßnahmen. Hier ist dann die Leitfrage, „Wie wird es gemacht?"

Schutzprofile für verschiedene Branchen

Eine weitere Neuerung, die sich nicht nur an kleinere Unternehmen richtet, sondern auch an Verwaltungen oder die Betreiber kritischer Infrastrukturen wie Wasserwerke: Für viele Branchen soll es spezielle, sofort umsetzbare Schutzprofile geben. Hier kann der IT-Grundschutz dann seine alte Stärke ausspielen, die konkrete technische Hilfe bei der Umsetzung von mehr IT-Sicherheit.

Solche Standardprofile sind eine Antwort auf ein Problem, das auch nach der Modernisierung bleiben wird: Die große Spreizung der Zielgruppen. „Beim BSI ist viel die Rede von kleinen Unternehmen wie Gewerbe- und Handwerksbetrieben", sagt Lutz Kolmey, Senior IT-Managementberater beim IT-Gesamtdienstleister Mod IT Services. „Das ist aber nicht der klassische Mittelstand und auch kein Markt für IT-Services."

Nach seinen Erfahrungen haben mittelständische Unternehmen im Moment vor allen Dingen erhöhten Bedarf bei Schwachstellenscans und beim Notfallmanagement. „Der typische Mittelständler möchte wissen, wo seine Lücken in der IT sind und was er tun muss, um ein vernünftiges Notfallmanagement aufzusetzen." Er sieht hier weiterhin hohen Beratungsbedarf. „Trotz der gesunkenen Komplexität sollten erfahrene Berater die Einführung des modernisierten IT-Grundschutzes begleitet werden, insbesondere wenn Technologien eingesetzt werden, für die es keine Empfehlungen im IT-Grundschutz gibt oder wenn sich bei einem höheren Schutzbedarf eine ergänzende Risikoanalyse empfiehlt", betont Lutz Kolmey. ●

Maria Urban
Journalistin in Berlin