secunet

IT-Grundschutz als automatisierter Prozess

Ohne leistungsfähige Informationstechnologie ist Polizeiarbeit heute undenkbar. Daher betreibt die Bundespolizei eine der größten polizeilichen IT-Landschaften Deutschlands. Ihrer Verpflichtung zum IT-Grundschutz kommt die Sicherheitsbehörde durch eine automatisierte Lösung nach, die den damit verbundenen Aufwand drastisch reduziert – und zudem die Sicherheit weiter erhöht

Aufgrund des 2007 vom Bundeskabinett verabschiedeten „Umsetzungsplans für die Gewährleistung der IT-Sicherheit in der Bundesverwaltung“ (UP Bund) ist die Bundespolizei verpflichtet, für jedes Fachverfahren ein sogenanntes IT-Sicherheitskonzept auf Basis des IT-Grundschutzes nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu erstellen. Dies ist einerseits folgerichtig, da für eine Sicherheitsbehörde naturgemäß hohe Anforderungen an die Informationssicherheit gelten müssen. Andererseits betreibt die Bundespolizei eine hochkomplexe IT-Infrastruktur mit rund 250 Fachverfahren an mehreren Standorten. Schnell war klar, dass sich die Erstellung und Pflege der Sicherheitskonzepte mit den zur Verfügung stehenden Ressourcen nicht in der herkömmlichen Vorgehensweise bewerkstelligen ließ.

Vor diesem Hintergrund entschied sich die Bundespolizei für einen neuen Ansatz: eine Lösung, die eine weitgehend toolgestützte Umsetzungsprüfung der Maßnahmen und Erstellung der IT-Sicherheitskonzepte ermöglicht. In secunet fand sie einen Partner, der aufgrund seiner langjährigen Projekterfahrung im Bereich IT-Grundschutz gut geeignet war, um ein solches Gesamtkonzept mitzuentwickeln. secunet ist seit Beginn der Konzeptionsphase im Jahr 2014 bis heute für fachliche Beratung, Sicherstellung der BSI-Konformität und Qualitätssicherung zuständig. Als weiterer Partner war Hewlett Packard Enterprise mit der Unterstützung der Konzeption und Systemintegration betraut.

Um eine weitgehend automatisierte Umsetzungsprüfung zu ermöglichen, wurden die Sicherheitsvorgaben für die IT-Infrastruktur stark vereinheitlicht: Die Sicherheitsmaßnahmen werden nun nicht mehr für jedes Fachverfahren separat, sondern für den Gesamt-Informationsverbund der Bundespolizei einheitlich festgelegt, umgesetzt, geprüft und dokumentiert. Dadurch entsteht eine sichere Kern-IT aus weitestgehend standardisierten Komponenten, die für unterschiedliche Fachverfahren genutzt wird.

Ein weiterer Kernaspekt für die Automatisierung ist die Modularisierung: An die Stelle der ansonsten im IT-Grundschutz üblichen „Bausteine“ treten Sicherheitsmodule (SiM). Genau wie die Bausteine modellieren die SiM die Zielobjekte des IT-Verbundes wie Systeme, Anwendungen, Netzwerk- oder Infrastrukturelemente und ordnen ihnen die jeweils vorgesehenen Maßnahmen zu. Allerdings werden die Maßnahmen der IT-Grundschutzkataloge durch zusätzliche erweitert, die auf Hersteller- und anderen Best-Practice-Empfehlungen basieren und für einen höheren Schutzbedarf gelten. Zudem sind die SiM viel stärker konkretisiert als die Grundschutzbausteine und legen auch jeweils die Prüfungen zur Umsetzung der Maßnahme fest. Dadurch lässt sich ein toolgestützter Basis-Sicherheitscheck der Maßnahmenumsetzung realisieren.

Diese automatisierte Umsetzungsprüfung erfolgt durch die Control Compliance Suite (CCS) von Symantec, die dazu auf Basis der Vorgaben aus den SiM entsprechende Informationen von den Systemen und Anwendungen sammelt und auswertet. Da diese technischen Checks nur für einen Teil der Maßnahmen möglich sind, werden sie durch webbasierte Multiple-Choice-Fragebögen ergänzt, die von den zuständigen Mitarbeitern (z. B. den Systemadministratoren) selbstständig ausgefüllt werden. Im Vergleich zur herkömmlichen Methodik der Umsetzungsprüfung mittels Interviews und Inspektion der Systemkonfigurationen ergibt sich daraus eine deutliche Zeit-, Kosten- und Ressourcenersparnis. Gleichzeitig sorgt die wesentlich detailliertere Prüfung für einen erheblichen Sicherheitsgewinn.

Die zentrale Verwaltung aller Informationen zu den Zielobjekten und Sicherheitsmaßnahmen sowie die automatische Erstellung der Sicherheitskonzepte erfolgt in einem neuen Software-Produkt von secunet, der Sicherheitsmanagement-Datenbank (SMDB). Diese importiert zum einen aus der CCS die Informationen zu den Zielobjekten und zum Umsetzungsstand der Sicherheitsmaßnahmen. Zum anderen ermöglicht sie über ein Web-Interface eine benutzerfreundliche Eingabe und Pflege aller weiteren Informationen zu den Fachverfahren, inklusive der Zuordnung der Zielobjekte zum jeweiligen IT-Verbund, der Netzpläne und Kommunikationsbeziehungen sowie der Risikoanalysen.

Der Pilotbetrieb der neuen Lösung hat bereits begonnen. Nach und nach werden alle Komponenten integriert, bevor die Lösung im Laufe des kommenden Jahres in den Wirkbetrieb übergehen soll. Die ersten Ergebnisse sind positiv: Beim Audit eines Fachverfahrens nach ISO 27001 auf Basis des IT-Grundschutzes stellten die Prüfer eine deutliche Verbesserung des Sicherheitsniveaus fest und gaben ein positives Feedback zum Konzept des automatisierten Grundschutzes. ■

Mehr Informationen:
Mario Tönse
mario.toense@secunet.com