

IT-Sicherheit nach BSI-Anforderungen

Fit für den IT-Grundschatz 2020 – mit digitaler Hilfe

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) überarbeitet jedes Jahr das IT-Grundschatzkompendium, um es an aktuelle Gefährdungen und IT-Produkte anzupassen. Dies bedeutet mitunter einen hohen Aufwand für die Behörden und Unternehmen, die den Grundschatz anwenden. Sie müssen ihre Maßnahmen an die Neuerungen anpassen und dies in ihren Sicherheitskonzepten dokumentieren. **secunet compass, die Lösung für den automatisierten IT-Grundschatz, hält nun Funktionen bereit, die diese Migration erheblich erleichtern. Zudem können die Anwender den Stand der Migration und das Sicherheitsniveau ihrer IT-Infrastruktur durch übersichtliche Reports für IT-Sicherheitsbeauftragte und Management jederzeit im Auge behalten. Die Bundespolizei, die bereits seit 2017 auf secunet compass vertraut, setzt die neuen Funktionen erfolgreich ein.**

Mit dem IT-Grundschatz des BSI können Behörden und Unternehmen ihr Sicherheitsniveau effektiv und nachweisbar erhöhen. Teil der bewährten Methodik ist es, für eine Vielzahl von „Informationsverbänden“ Sicherheitskonzepte zu erstellen und deren Umsetzung kontinuierlich zu überprüfen. Allerdings führen immer komplexere und schnelllebige IT-Infrastrukturen zu einem erhöhten Aufwand für den IT-Grundschatz: Immer mehr Sicherheitskonzepte müssen erstellt werden, und kaum ist das erledigt, sind sie schon wieder überholt. Um den Ressourceneinsatz dennoch in angemessenen Grenzen zu halten, setzt die Bundespolizei seit 2017 mit secunet compass den IT-Grundschatz weitgehend automatisiert um. Auch für andere Behörden und Unternehmen ist die Lösung verfügbar.

secunet compass ermöglicht es, Informationssicherheit nach den Vorgaben des IT-Grundschatzes Toolgestützt zu etablieren. Die Lösung prüft technische Komponenten automatisiert und erstellt vollständige IT-Sicherheitskonzepte nach den Anforderungen des BSI. Kernstück sind dabei die sogenannten Sicherheitsmodule. Sie beziehen sich auf die Anforderungen der Bausteine des IT-Grundschatzkompendiums für verschiedene Zielobjekte wie etwa Systeme und Anwendungen. Diese Anforderungen sind im IT-Grundschatzkompendium recht allgemein gehalten. Die Sicherheitsmodule konkretisieren sie, und zwar auf der Grundlage von Best-Practice- und Härtings-Empfehlungen.

Wo möglich, werden die Anforderungen auf detaillierte Konfigurationseinstellungen einzelner Produkte abgebildet, so dass sie mit einer Compliance-Software vollautomatisch geprüft werden können. Die Umsetzung von nicht technisch prüfbar Anforderungen wird in einer Web-Anwendung durch Fragebögen mit Multiple-Choice-Antworten erfasst.



 Die Bundespolizei vertraut bereits seit 2017 auf **secunet compass**.

jene Anforderungen, die sich nicht geändert haben, die Ergebnisse der Umsetzungsprüfung automatisch übernommen. Für alle geänderten Anforderungen werden die alten und neuen Prüffragen sowie die Ergebnisse der Umsetzungsprüfung übersichtlich nebeneinander gestellt. Für jede Anforderung kann der Anwender dann entscheiden, ob er die Prüfergebnisse übernehmen will oder nicht. Nach diesem Migrationsschritt muss nur noch die Umsetzung der neu hinzugekommenen Anforderungen sowie von geänderten Anforderungen, für welche die Prüfergebnisse nicht übernommen worden sind, geprüft werden. Bei technisch prüfbar Anforderungen kann diese Prüfung sogar vollautomatisch erfolgen.

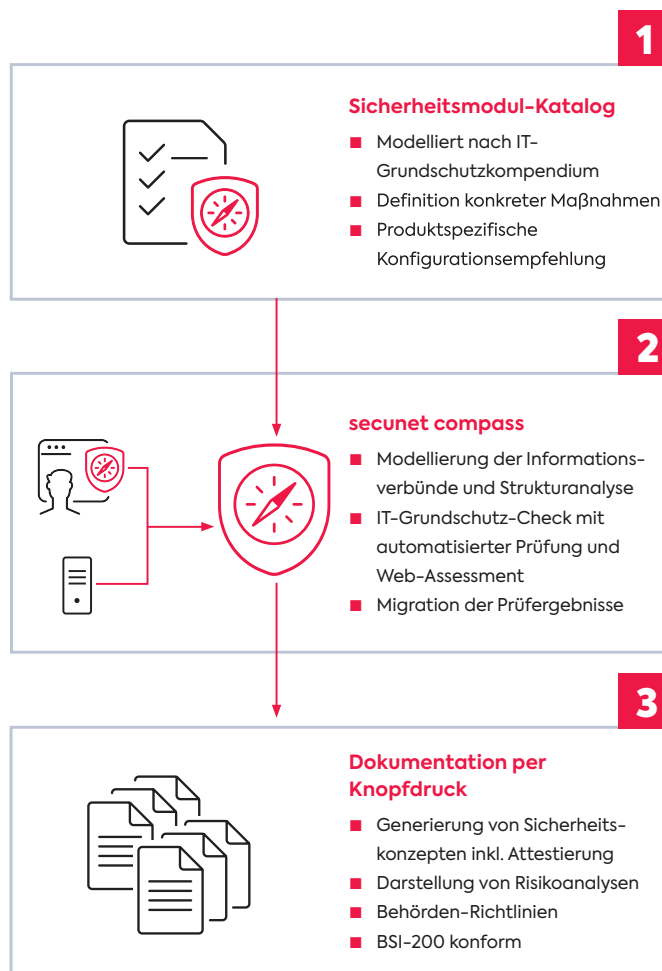
Über eine feingranulare Rollen- und Rechteverwaltung können die Fragebögen an unterschiedliche Gruppen und Personen delegiert werden. Die Ergebnisse der Umsetzungsprüfung können dann auf Knopfdruck in einem Sicherheitskonzept dokumentiert werden. Aktuell stehen in **secunet compass** über 90 Sicherheitsmodule für die verschiedensten Produkte und Aspekte zur Verfügung und dieser Katalog wird unter Einbeziehung der Kunden kontinuierlich erweitert.

Da sich die IT jedoch beständig weiterentwickelt – und mit ihr die Bedrohungslage –, müssen die umgesetzten Sicherheitsmaßnahmen laufend an die veränderten Gefährdungen und aktuellen Produkte angepasst werden. Das BSI aktualisiert daher jedes Jahr die im IT-Grundschutzkompendium enthaltenen Bausteine. In der aktuellen Edition 2020 wurden zahlreiche Anforderungen geändert, hinzugefügt oder entfernt. Zudem enthält sie zwei neue Bausteine. **secunet compass** hat die Anpassungen der Edition 2020 bereits in den Sicherheitsmodulen nachvollzogen und ist somit auf dem neuesten Stand.

Für Anwender des IT-Grundschutzes stellt die regelmäßige Aktualisierung der Anforderungen allerdings eine Herausforderung dar: Die zuvor mit viel Aufwand erhobenen Informationen zur Umsetzung müssen für alle Zielobjekte entweder von Grund auf neu erhoben oder manuell auf die geänderten Anforderungen übertragen werden. Die Ressourcen, die für diese Migration erforderlich sind, fehlen dann oft an anderer Stelle, z. B. bei der Umsetzung dringender Maßnahmen oder der Realisierung wichtiger Projekte.

Um den Aufwand für die Migration zu minimieren, bietet **secunet compass** eine Funktion zur Übertragung der bestehenden Prüfergebnisse und Antworten auf die neuen Sicherheitsmodule. Dabei werden für

Die Funktion zur Übernahme der Prüfergebnisse reduziert den Aufwand für die Umsetzungsprüfung auf ein Minimum. Trotzdem kann es notwendig sein,



für neue oder geänderte Anforderungen zusätzliche Maßnahmen umzusetzen. secunet compass bietet hierfür geeignete Funktionen zur Planung der Umsetzung, inklusive der Termine, Verantwortlichkeiten und Kosten.

Der aktuelle Stand der Umsetzung, und damit auch das aktuell erreichte Sicherheitsniveau, kann nicht nur im IT-Sicherheitskonzept eingesehen werden, sondern ist auch auf einen Blick in verschiedenen Reporting-Ansichten für die einzelnen Informationsverbände erkennbar. Dabei stellen farbige Diagramme übersichtlich dar, welcher Anteil der Anforderungen umgesetzt wurde, nicht umgesetzt wurde, entbehrlich ist oder noch nicht geprüft wurde. In den Reports für den IT-Sicherheitsbeauftragten wird der Umsetzungsgrad für jedes Sicherheitsmodul

und zusammengefasst für jede IT-Grundschutz-Schicht dargestellt. Der Management-Report verdichtet die Anzeige stärker und fasst den Stand der Umsetzung für Anforderungen an Prozesse und Systeme zusammen.

Durch die Reporting-Ansichten können die verantwortlichen Mitarbeiter jederzeit den Umsetzungsstand nachverfolgen und erkennen, wo die größten Baustellen liegen. Somit behalten sie stets den Überblick über das aktuelle Sicherheitsniveau ihrer Informationsverbände und können die Maßnahmen, die noch umgesetzt werden müssen, optimal priorisieren.



Johannes Merkle
johannes.merkle@secunet.com



BUNDESPOLIZEI

„secunet compass ist für die Bundespolizei ein essentielles Werkzeug zur Etablierung eines einheitlichen Sicherheitsniveaus. Die Sicherheitsmodule schärfen die allgemeinen Anforderungen des IT-Grundschutzes und unterstützen somit die adressatengerechte Umsetzung innerhalb unserer dezentralen Organisation mit ihrer heterogenen Infrastruktur. Dank der neuen Visualisierungsfunktionen in secunet compass können wir den aktuellen Umsetzungsgrad des Sicherheitsniveaus umgehend erfassen und wichtige Kennzahlen als Grundlage weiterer Planungen ermitteln.“

Thomas Schonhof, Bundespolizei