Vorteile durch Standardisierung und verteiltes Arbeiten

Grundschutz as a Service

Mit Standardisierung, redundanzfreien Sicherheitskonzepten und vereinfachtem Zusammenarbeiten lassen sich heterogene IT-Landschaften, komplexe Organisationsstrukturen und straffe Zeitpläne meistern.

Von Steffen Voigt, HiScout

Das IT-Sicherheitsgesetz kennt mittlerweile jeder Verantwortliche in den Behörden und Kommunen. Aber lange noch nicht alle Verwaltungen erfüllen die Anforderungen des Gesetzes und treiben das Thema IT-Sicherheit mit der notwendigen Entschiedenheit voran. Während Behörden, die sich der Materie rechtzeitig widmeten und die notwendigen Ressourcen zur Verfügung hatten, längst zertifizierungsfähig oder zertifiziert sind, stehen gerade die kleinen Behörden und Kommunen teilweise noch am Anfang.

Historisch gewachsene, heterogene IT-Landschaften gehören dabei zu den großen Herausforderungen. Sie sind nicht selten dezentral organisiert, über mehrere Städte oder sogar Bundesländer verteilt. Hinzu kommen komplexe Organisationsstrukturen, in denen häufig ausgeprägte Rollen- und Rechtekonzepte fehlen. Manchmal herrscht auch ein gewisser „Daten-Egoismus“ vor, der Datenzugriffe nur auf den „eigenen Bereich“ beschränkt sehen will. Übergreifende Zusammenarbeit wird dadurch erschwert und Redundanzen in der Datenhaltung Vorschub geleistet.

Nicht zuletzt drängt die Zeit, um die Infrastrukturen gemäß den Anforderungen des IT-Sicherheitsgesetzes und – wo erforderlich – der BSI-Kritisverordnung anzupassen.

Mangelnde Ressourcen und schwieriger Einstieg

Kommunen sind angesichts heterogener IT-Umgebungen und fehlender Rollenkonzepte bei der Umsetzung des Grundschutzes oft vor nicht minder große Probleme gestellt. Hinzu kommen zumeist eine dünne Personaldecke und knappes Geld. Groß ist die Angst, dass schmale Budgets für die falschen Dinge ausgegeben werden könnten.

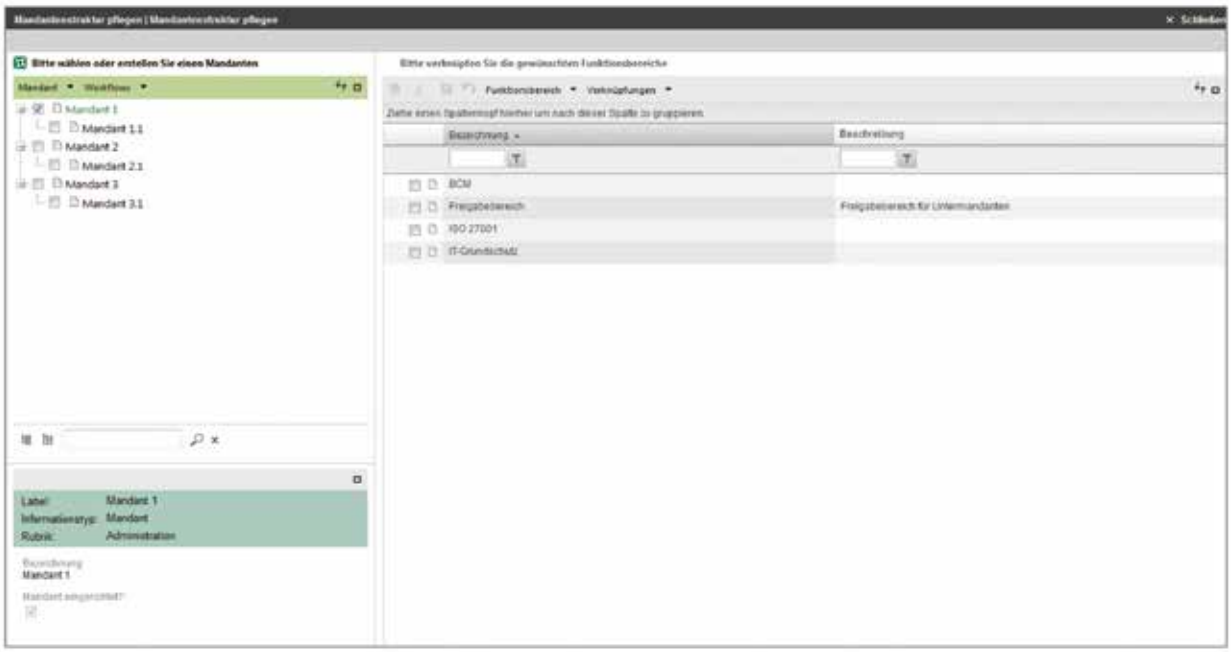

Abbildung 1: Über eine einfache Objekthierarchie können die gesamte Organisationsstruktur abgebildet und jedem Mandanten die erforderlichen Funktionsbereiche zugeordnet werden. Auf dieser Grundlage erfolgt die Einrichtung der entsprechenden Datenablagen und Berechtigungsgruppen automatisiert.

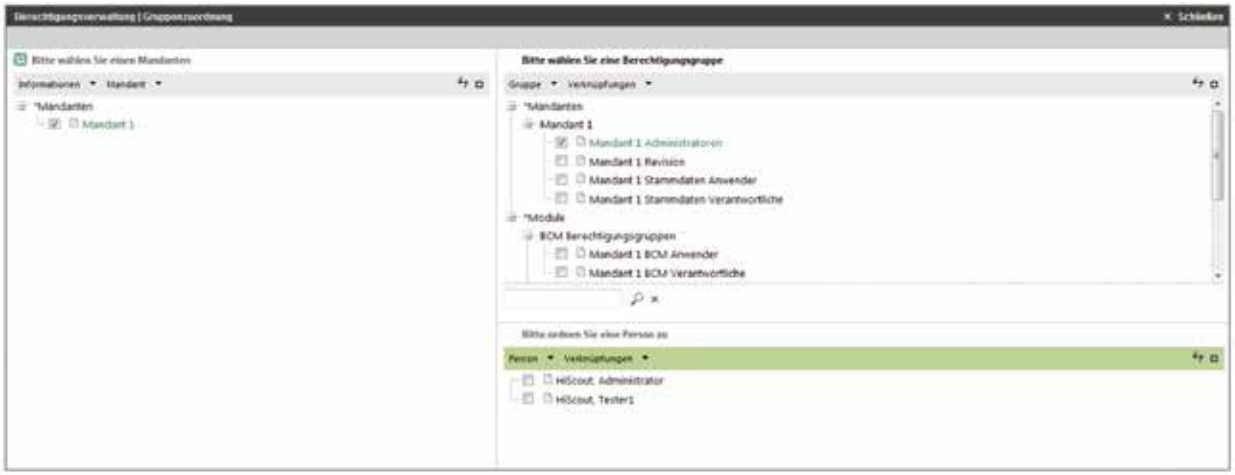

Abbildung 2: Jeder Mandant erhält automatisch ein Basis-Set an Berechtigungen. Es müssen lediglich User zu den entsprechenden Berechtigungsgruppen hinzugefügt werden.

Mitarbeitern, die eigentlich ein ganz anderes Sachgebiet bearbeiten, wird aufgrund der Personalsituation nicht selten quasi nebenbei die Mitverantwortung für die IT-Sicherheit übertragen. Sie haben in der Regel wenig Erfahrung in der Materie, sehen sich aber mit der Aufgabe konfrontiert, möglichst von heute auf morgen den IT-Grundschutz in den kommunalen Verwaltungen einzuführen. Es macht die Sache nicht leichter, dass die Menge der Tool-Anbieter verwirrend ist. Wie das geeignete Tool finden und dabei unnütze Lehrgeld-Zahlungen vermeiden? Alles zusammengenommen stellt sich der Einstieg für Kommunen in der Tat als recht schwierig dar.

Aktualisierter Grundschutz für schnelleren Einstieg

Das BSI als zuständige Behörde versucht diesbezüglich mit verschiedenen Vorgehensweisen und Grundschutzprofilen zu unterstützen. So bildet der BSI-Standard 200-2 die Basis der bewährten BSI-Methodik zum Aufbau eines soliden Informationssicherheitsmanagements (ISMS). Er etabliert drei Vorgehensweisen bei der Umsetzung des IT-Grundschutzes: Die Basis-Absicherung liefert einen Einstieg zur Initiierung eines ISMS. Mit der Standard-Absicherung kann ein kompletter Sicherheitsprozess implementiert werden. Die Kern-Absicherung ist die Vorgehensweise zum Einstieg in ein ISMS, bei der zunächst ein Teil eines größeren Informationsverbundes betrachtet wird.

Auf der Webseite des BSI lassen sich des Weiteren IT-Grundschutzprofile herunterladen, beispielsweise zur Basis-Absicherung Kommunalverwaltung. Der Einstieg wird dadurch erleichtert, aber ein Kernproblem bleibt: Das GSTOOL für den IT-Grundschutz bietet das BSI nicht mehr an, sondern verweist an dieser Stelle auf über 20 Anbieter als Alternative. Leider kann die Behörde aus rechtlichen Gründen bei der Auflistung keine Empfehlung aussprechen.

Wie können die Toolhersteller helfen

Auch die Toolhersteller können ihrerseits dafür sorgen, den Einstieg für Organisationen so einfach wie möglich zu gestalten. Beispielsweise ist die HiScout GmbH schon lange Akteur bei der toolseitigen Unterstützung der Umsetzung des IT-Grundschutzes in Unternehmen, Behörden und Kommunen. Häufig sind es die gleichen Problemstellungen, vor denen Unternehmen und Verwaltungen stehen. Insbesondere geht es um das Beherrschen der Zusammenarbeit in verteilten Organisationen. In vielen Projekten bei größeren Unternehmen und in Behörden jeglicher Größe wird beim Customizing relativ viel Zeit für das Erstellen des Berechtigungssystems verwendet. Der Prozess des Abbildens von Mandanten, Fachbereichen und des Einrichtens von verschiedenen Rollen für die unterschiedlichen Zugriffsmöglichkeiten auf die Daten ähnelt sich in den Projekten recht häufig.

HiScout hat diese und andere Erfahrungen aus zahlreichen, auch sehr großen Behördenprojekten als Best Practice in der HiScout GRC Suite gebündelt einfließen lassen. Entstanden ist die Lösung HiScout Behördenstandard, welche auf die Anforderungen der meisten Behörden fokussiert.

Mit der Lösung kann ein Berechtigungs- und Mandantenkonzept einfach konfiguriert und automatisiert eingerichtet werden (Abb. 1). Zu jedem Mandanten gibt es ein definiertes Set an Berechtigungen, mit dem die Kunden sofort arbeiten können (Abb. 2).

Wesentlicher Bestandteil zahlreicher Projekte war die Unterstützung der Zusammenarbeit in verteilten Organisationen. HiScout kann nun bereits im Standard mit Services, Produktzielobjekten und Referenzierungen umgehen. Bereits vorhandene Informationen können besser genutzt und wiederverwendet werden, um schneller redundanzfreie Sicherheitskonzepte zu erstellen (Abb. 3).

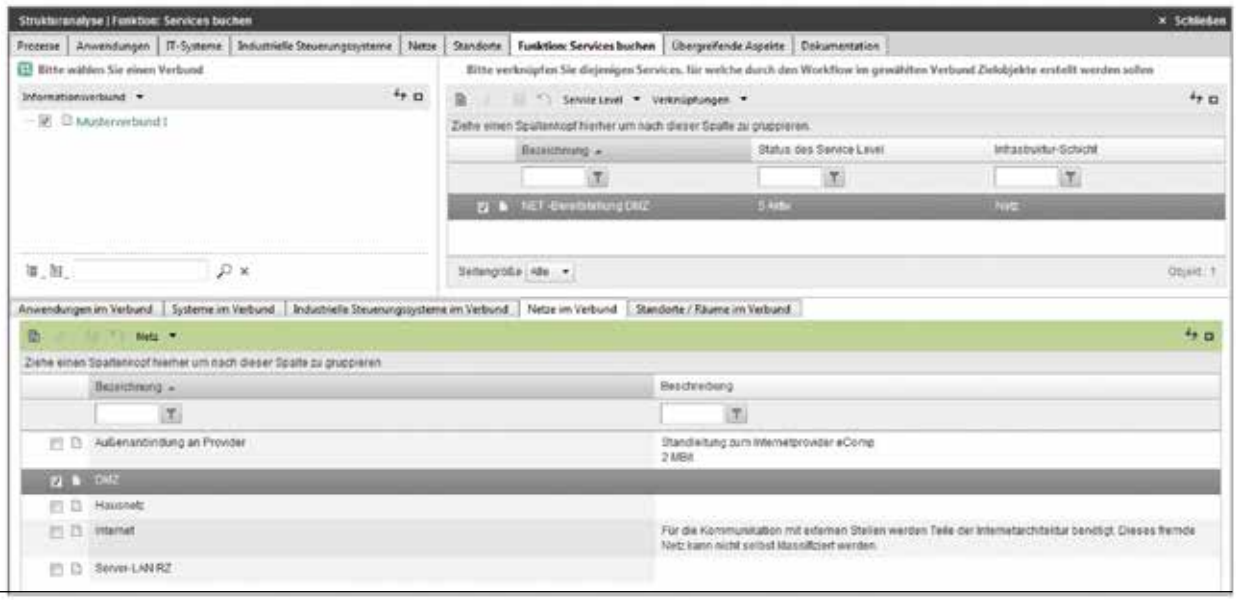

Abbildung 3: In der Strukturanalyse können Services gebucht werden, die zum Beispiel auf Basis-IT verweisen. Die Bereitstellung von Zielobjekten durch einen anderen Bereich kann so abgebildet werden.

Durch die Erweiterungen in der HiScout GRC Suite können zahlreiche kundenspezifische Anpassungen entfallen, die bisher für den Einstieg notwendig waren. Zusätzliches Customizing über den Standard hinaus sind natürlich weiterhin möglich.

Öffentliche Rechenzentren als Service-Dienstleister und Mittler

Das BSI und die Toolhersteller allein können selbstverständlich nicht allen eingangs geschilderten Herausforderungen begegnen. Gerade kleine Kommunen sind häufig überfordert, weil sich derartige Projekte nur schwer allein stemmen lassen. Wie sollen sie aus dem Angebotswirrwarr die richtige und zudem kostengünstige Lösung für ihre Verwaltung finden? Den Kommunen bleibt die Hoffnung, dass die öffentlichen Rechenzentren sich dafür in der Pflicht sehen. Als Partner könnten diese ein einheitliches Verfahren für IT-Sicherheit bei Behörden und Kommunen anbieten. Wenn man so will: IT-Grundschutz as a Service.

Die Vorteile für ein vereinheitlichtes Verfahren liegen auf der Hand. Die Verwaltungen haben einen Ansprechpartner für ihre Problemstellungen, bei dem sie ohnehin schon Kunde sind. Sie sparen enorm Aufwand bei der Tool-Auswahl und bei der Vorgehensweise, vermeiden Fehler und Anlaufverluste. Und eine Lösung wird sehr schnell zur Verfügung gestellt.

Auch volkswirtschaftlich gesehen ist diese Herangehensweise optimal, denn nicht jede Behörde und Kommune müsste ihren Prozess selbst ermitteln und etablieren.

Die Rechenzentren wären zugleich Partner und Mittler zwischen Behörden und Kommunen einerseits und den Tool-Anbietern andererseits. Rechenzentren könnten so auch einen intensiven Erfahrungsaustausch anstoßen und eventuell mit weiteren Partnern standardisierte Schulungen für Anwender anbieten.

Aus technischer Sicht übt das Rechenzentrum die Rolle eines Hauptmandanten aus, der die bereitgestellten Zielobjekte pflegt. Die Kunden benötigen dann nur eine Referenz in ihr Sicherheitskonzept. Voraussetzung für eine derartige Lösung sind natürlich einheitliche Werkzeuge, die diese Arbeitsweise unterstützen, entsprechende Schnittstellen und ein mandantenfähiges Tool.

Fazit

Die Gefahr ist erkannt, aber noch nicht gebannt. Die Voraussetzungen für die schnelle Etablierung des IT-Grundschutzes in Behörden und Kommunen sind jedoch vorhanden. Jetzt sind alle Akteure – Behörden, Kommunen, Rechenzentren und Tool-Hersteller – gefordert, in einen effektiven Dialog zu treten, wobei die Rechenzentren als zentrale Mittel- und Anlaufpunkte fungieren sollten. ■

Steffen Voigt ist Produktverantwortlicher bei der HiScout GmbH.