Grundschutz, Datenschutz, Notfallmanagement

Drei auf einen Streich!

Dieser Artikel möchte Behörden und Kommunen eine Checkliste für die Nutzung von Synergien bei Beschaffung, Einrichtung, Customizing und Datenpflege von Managementsystemen an die Hand geben. Damit können sie bei Investitionsentscheidungen die Optimierung von Arbeitsaufwand und Kosten besser in den Fokus nehmen.

Von Michael Langhoff, HiScout GmbH

©Jirsak – shutterstock.com

Die Corona-Krise zeigt, dass modellierte Risikoszenarien nicht nur theoretische Überlegungen sind, sondern im realen Leben wirklich eintreffen. Fehlende Notfallpläne können schwerwiegende Konsequenzen haben und zu menschlichen und wirtschaftlichen Verlusten führen. Das Bewusstsein, dass es in der eigenen Organisation dringenden Handlungsbedarf gibt, trifft heute schmerzlich mit einer Verknappung finanzieller und personeller Ressourcen zusammen. Finanzhilfen zur Bewältigung wirtschaftlicher Notlagen und ausbleibende Steuereinnahmen werden die öffentlichen Kassen auf Jahre hinaus belasten und den finanziellen Spielraum von Behörden und Kommunen erheblich einschränken.

Hinzu kommen personelle Engpässe. Diese sind Vorboten einer der Alterspyramide folgenden wachsenden Personalknappheit. Aus der Not heraus werden Mitarbeiter mit Themen der Informationssicherheit betraut, die andere Hauptaufgaben haben und nicht oder nur unzulänglich für die zu verantwortenden Themen ausgebildet sind.

Auch die organisatorische und technische Situation stellt sich vielerorts äußerst kompliziert dar. Die IT-Landschaften sind häufig historisch gewachsen, heterogen und über mehrere Städte oder Bundesländer verteilt. Die vorhandenen Rollen- und Rechtekonzepte sind oft zu unausgereift für die komplexen Organisationsstrukturen.

Wie können öffentliche Institutionen in dieser schwierigen Situation schnell und zielorientiert nachhaltige Investitionen tätigen? Wie lassen sich durch Nutzung von Synergien Zeit und Kosten bei der Einführung und dem Betrieb von Managementsystemen sparen?

Mehrere Organisationen verwenden die gleiche Software

Die gemeinsame Beschaffung oder Verwendung einer in vergleichbaren Organisationen bereits etablierten Lösung spart Zeit für die Tool-Auswahl und die Festlegung der Vorgehensweise. Nachfolgende Behörden können Fehler und Anlaufschwierigkeiten der Vorreiter vermeiden und treten schnell in die Phase produktiver Anwendung ein. Mit dieser Zielsetzung hat zum Beispiel die Landesoberbehörde IT Baden-Württemberg (BITBW) einen Rahmenvertrag zur Einführung der HiScout GRC Suite an allen Standorten der Landesverwaltung geschlossen.

Auch im laufenden Betrieb tragen behördenübergreifende Ansprechpartner zur effektiven Verwaltung und Personaleinsparung bei. Anwendergruppen, wie die HiScout User Group „Öffentliche Verwaltung“, treffen sich regelmäßig zum Erfahrungsaustausch und stimmen sinnvolle Standards miteinander ab. Gemeinsame Anwenderschulungen schonen die knappen Ressourcen.

Mehrere Organisationen verwenden eine gemeinsame IT-Infrastruktur

Kommunale, behördliche und privatwirtschaftlich betriebene Rechenzentren können die Komponenten Grundschutz, Datenschutz und Notfallmanagement der GRC-Software als „Software as a Service (SaaS)“ zur gemeinsamen Nutzung

durch mehrere Organisationen bereitstellen. Das ITZBund stellt beispielsweise unter dem Namen ZeDIS allen Bundesbehörden ausgewählte Module der HiScout GRC Suite als SaaS-Lösung zur Verfügung. Teilnehmende Behörden buchen standardisierte Infrastrukturkomponenten, wie zum Beispiel einen „virtuellen Windows-Server" oder ein „Datenbank-Cluster" des Rechenzentrums, woraufhin die entsprechenden Zielobjekte automatisch in die eigenen Sicherheitskonzepte eingebunden werden.

Verwendung eines vorkonfigurierten Softwaresystems

Der große Vorteil einer Standardsoftware liegt darin, dass Funktionen, Abläufe und Inhalte bereits im Sinne des Anwenders vorgedacht und konfiguriert sind. Im HiScout Berechtigungssystem sind Rollen bereits mit ihren typischen Zugriffsmöglichkeiten ausgestattet. Beim Anlegen von Mandanten und Fachbereichen werden Datenablage und Berechtigungen automatisch eingerichtet. Die Verantwortlichen müssen den bereitgestellten Nutzergruppen nur noch ihre individuellen User hinzufügen. Komplexe Organisationsstrukturen werden mit einem differenziert zu konfigurierenden Mandanten-Management präzise nachgebildet. Dabei ist eine vollständige Trennung oder übergreifende Nutzung von Stammdaten möglich. Das beschriebene Vorgehen ist in Organisationsstrukturen mit bis zu dreistelligen Untereinheiten erfolgreich im Einsatz. Auch fachliche Inhalte zum Grundschutz, Datenschutz und Notfallmanagement sind bereits enthalten.

Verwendung eines auf Kommunen und Behörden spezialisierten Systems

HiScout hat die Best Practices und etablierten Anwendungsroutinen vieler Bundes- und Landesbehörden integriert und steht in ständigem Austausch mit diesen Stakeholdern. Eine weitere User Group für Kommunen wird zurzeit eingerichtet. Neue Anwender profitieren davon, dass die Anforderungen zahlreicher Nutzer mit ähnlichen Bedürfnissen bereits in die Standardsoftware eingeflossen sind und nicht mehr in einem aufwendigen Customizing-Verfahren ergänzt werden müssen. Auch die kontinuierliche Weiterentwicklung richtet sich an den Bedürfnissen der Anwender aus.

Verwendung eines gemeinsamen Datenpools für Grundschutz, Datenschutz und Notfallmanagement

In einem integrierten Managementsystem für verschiedene Sicherheitsthemen können vorhandene Informationen gemeinsam genutzt und redundanzfreie Sicherheitskonzepte, Verfahrensverzeichnisse und Notfallkonzepte erstellt werden. Bei HiScout steht es den Anwendern frei, in welchem Modul die Stammdaten der Organisation erfasst und gepflegt werden. Alle Ergänzungen und Änderungen fließen in der gemeinsamen Datenbasis zusammen.

Folgendes Beispiel soll die möglichen Synergieeffekte und Zeitersparnisse verdeutlichen: Der Grundschützer beginnt mit der Arbeit und erhebt Prozesse und benötigte Anwendungen. Der Notfallmanager freut sich über die bereits erhobenen Daten und verwendet sie für die Business-Impact-Analyse. Währenddessen nutzt der Datenschützer die bereits gepflegten Stammdaten, um im Verzeichnis der Verarbeitungstätigkeiten zu erheben, welche Daten durch welche Anwendungen verarbeitet werden. Diese Informationen kann der Grundschützer wieder in seine Prozessbetrachtung für die Schutzbedarfsfeststellung einfließen lassen.

Die Umsetzbarkeit zukünftiger Anforderungen sicherstellen

Kommen neue Anforderungen auf die Organisationen zu, zum Beispiel die Einführung eines Geheimschutz-Management-Systems oder die Abbildung weiterer Security-Frameworks, wie OWASP, offenbart sich die Flexibilität und Zukunftsfähigkeit des genutzten Tools. Anwender der generischen HiScout-Technologie können das Datenmodell und die Benutzeroberfläche jederzeit auch ohne Programmierkenntnisse erweitern. Die Softwareinvestition ist zukunftssicher und führt nicht in eine Sackgasse.

Fazit

Bedingt durch die Corona-Krise und den Fachkräftemangel werden Kommunen und Behörden in den nächsten Jahren über geringe finanzielle und personelle Ressourcen verfügen. Gleichzeitig besteht ein großer rechtlicher, organisatorischer und faktischer Handlungsdruck zur Einführung und Optimierung von Managementsystemen für IT-Grundschutz, Datenschutz und Notfallmanagement.

Die geschickte Nutzung von Synergien zwischen verschiedenen Organisationen und Softwaretools trägt dazu bei, diese mit besserem Ergebnis zu nutzen und Aufwand und Kosten in einem vertretbaren Rahmen zu halten. Durch vorausschauende Berücksichtigung zukünftiger Anforderungen wird eine langfristige Nutzung der Systeme möglich.

Bei der Beschaffung sollten die entsprechenden Produktanforderungen vorab definiert werden und im Mittelpunkt der Entscheidungsprozesse stehen. Die HiScout GRC-Software (www.hiscout.com) erfüllt diese Kriterien durch langjährige Spezialisierung auf Behörden und Kommunen.