INSIMAT

Informations-Sicherheits-Management-Tool

für Risikomangement nach ISO 27001

in IT-Netzwerken

zur Strukturierung, Risikoeinschätzung, Risikoanalyse und Risikobehandlung

mit tabellarischer Darstellung und Überarbeitbarkeit sowie Eingabe-Formularen

anpassbar in den Algorithmen, Datenfeldern und Strukturen

auf Basis der Anwendungs-Entwicklungsplattform Ninox

Kontext

In Informations-Sicherheits-Projekten ist die Wahl eines geeigneten ISMS (Informations-Sicherheits-Management-System) einer der ersten Entscheidungen in einem ISMS-Projekt. Oft wird dieser Schritt noch vor der Netzstrukturierung und der Beschreibung des Analyseprozesses gemacht. Dies hat zur Folge, dass das Tool nicht zur Netzstruktur und dem Analyseprozess passt, und dadurch die Netzstruktur aufwändig und umständlich abgebildet und der Prozess den Möglichkeiten des ISMS angepasst werden muss. Die Effizienz und Akzeptanz des ISMS geht dabei verloren.

Viele Projekte starten daher mit Tabellenkalkulations- und Textverarbeitungs-Programmen. Dies ermöglicht eine zugeschnittene und schlanke Lösung und bietet viel Flexibilität und Agilität für die Zukunft. Mit zunehmenden Inhalten, Nutzern und weiteren Anwendungsfeldern treten jedoch auch die Nachteile solcher Lösungen in den Vordergrund, wie fehlende Versionierung, keine Backup-Mechanismen, limitierte Funktionalitäten und keine Mehrbenutzer-Fähigkeit.

Produkt

Der INSIMAT schlägt die Brücke von diesen einfachen Werkzeugen, hin zu einem Expertensystem für Risikomanagement (ISO27001 / IT-Sicherheitsgesetz). Er ist auf Basis der Anwendungs-Entwicklungsplattform Ninox (ninoxdb.de) programmiert worden.

Die verwendete Entwicklungsplattform Ninox (ninoxdb.de) erlaubt die Programmierung von Datenbankanwendungen mit Web-Front-End und ermöglicht eine tabellarische Darstellung und Bearbeitbarkeit, genauso wie die Eingabe über Formulare und Darstellung in Reports, Diagrammen und speziellen Ansichten. Zusätzlich zum Web-Interface bietet Ninox einen Zugang über Apps für iOS, Android und MacOS. Die Anwendung kann entweder in der Ninox-Public-Cloud laufen oder auf einem Server des Unternehmens oder eines dedizierten Hosters. Umfangreiche Funktionen und die Scripting-Sprache ermöglichen jeglichen Wunsch bei der Umsetzung eines Projektes.

Mit Hilfe dieser Funktionalitäten ist der INSIMAT aus einem ISMS-Projekt eines Fernleitungsnetzbetreibers heraus entstanden und kann nun von anderen Unternehmen erworben und bei Bedarf für sie angepasst werden. In der folgenden Tabelle Leistungsmerkmale sind alle wesentlichen Features beschrieben.

So wie die derzeitigen Leistungsmerkmale aus der Praxis eines exemplarischen Projektes heraus entstanden sind, werden sie gesteuert durch Anwenderwünsche auch weiterentwickelt und ergänzt. Hierzu ist ein Anwenderforum in Planung, in dem die Anwender sich über die Umsetzung der Informationssicherheit austauschen und auch die Roadmap des INSIMATs mit beeinflussen können.

Produktbeschreibung

Die Risikoanalysen werden für ein Strukturelement (z.B. Netz oder Organisation) angelegt. Dabei wird der Schaden und der Schutzbedarf für die Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) verwendet.

Die Ermittlung des Schadens und des Schutzbedarfes der Strukturelemente wird über eine Betrachtung der Geschäftsprozesse eingeschätzt und über die zugehörigen Informationen auf die Strukturelemente vererbt. Eine manuelle Anpassung ist dabei auf allen Ebenen möglich. Die Elemente können hierbei in einer Hierarchie abgebildet werden, so dass die Risikoanalyse auf verschiedenen Hierarchiestufen angewendet werden (z.B. für die Gruppe Übertragungstechnik oder eines spezielles Systems).

Eine dem Risiko entsprechende Gefährdung wird nun hinzugefügt. Die Auswirkung auf die Schutzziele ergibt in Verbindung mit dem Schutzbedarf des Strukturelements das Risiko pro Schutzziel.

Nun werden der Gefährdung die bereits getroffenen Maßnahmen entgegengesetzt. Deren Kompensationswirkung wird pro Schutzziel des Risikos berücksichtigt und ergibt das Restrisiko.

Diese Verminderung des Risikos geht als reduzierender Faktor in die Kalkulation der Risikokennzahl ein, die sich aus Eintrittswahrscheinlichkeit multipliziert mit dem Schaden berechnet.

Kataloge für Gefährdungen, Schadenskriterien, Verantwortlichkeiten und Maßnahmen stehen für alle Risikoanalysen zur Verfügung und ermöglichen eine effiziente Vorgehensweise.

Für hohe Risiken werden dann Risikobehandlungen abgeleitet, die zusätzlich reduzierende Maßnahmen implementieren und nach ihrer Umsetzung die entsprechenden Risiken weiter vermindern.

Der Informationssicherheitsbeauftragte und jeder Verantwortliche erhält über ein Dashboard eine Sicht auf die ihn betreffenden Risikoanalysen, Risikobehandlungen und Strukturelemente. Dieses Dashboard bietet auch eine statistische Auswertung pro Risikoniveau, Analysetiefe und über die Zeit.

Über ein optionales Module Workflow kann der PDCA-Prozess für Sicherheitsvorfälle, Verbesserungsmaßnahmen und Auditergebnisse gesteuert werden.

Ein weiteres optionales Modul Assetmanagement erlaubt die Verwaltung der Asset ausgehend von den Strukturelementen.

Ein Changemanagement-Modul kann für den Veränderungsprozess des Netzes ergänzt werden.

Alle Daten können in einer Formularsicht oder einer tabellarischen Sicht bearbeitet werden, in Reports übernommen oder in Excel exportiert werden.

Produktkonfiguration und Anpassungen

Der INSIMAT kann im Rahmen seiner Standard-Funktionalität konfiguriert werden und bei Bedarf individuell funktional angepasst oder erweitert werden. Kleine Anpassungen können direkt in der laufenden Anwendung vorgenommen werden, für größere Änderungen empfiehlt sich eine Offline-Entwicklung und Implementierung innerhalb eines Wartungsfensters.

Installation und Betrieb

Der INSIMAT basiert auf der Anwendungs-Entwicklungsplattform Ninox und benötigt daher eine Ninox-Installation, die entweder auf einem Server (Windows) des Unternehmens oder in einer Private Cloud (dedizierter Server eines Hosters) betrieben werden. Das Frontend ist Browser- und App-basiert. Apps werden für Android, iOS und MacOS angeboten, die auch offline genutzt werden können oder als Einzelarbeitsplatz-Lösung verwendet werden können. Die Nutzung der Ninox Cloud (public) wird aufgrund der Bearbeitung von sensiblen Sicherheitsdaten nicht empfohlen.

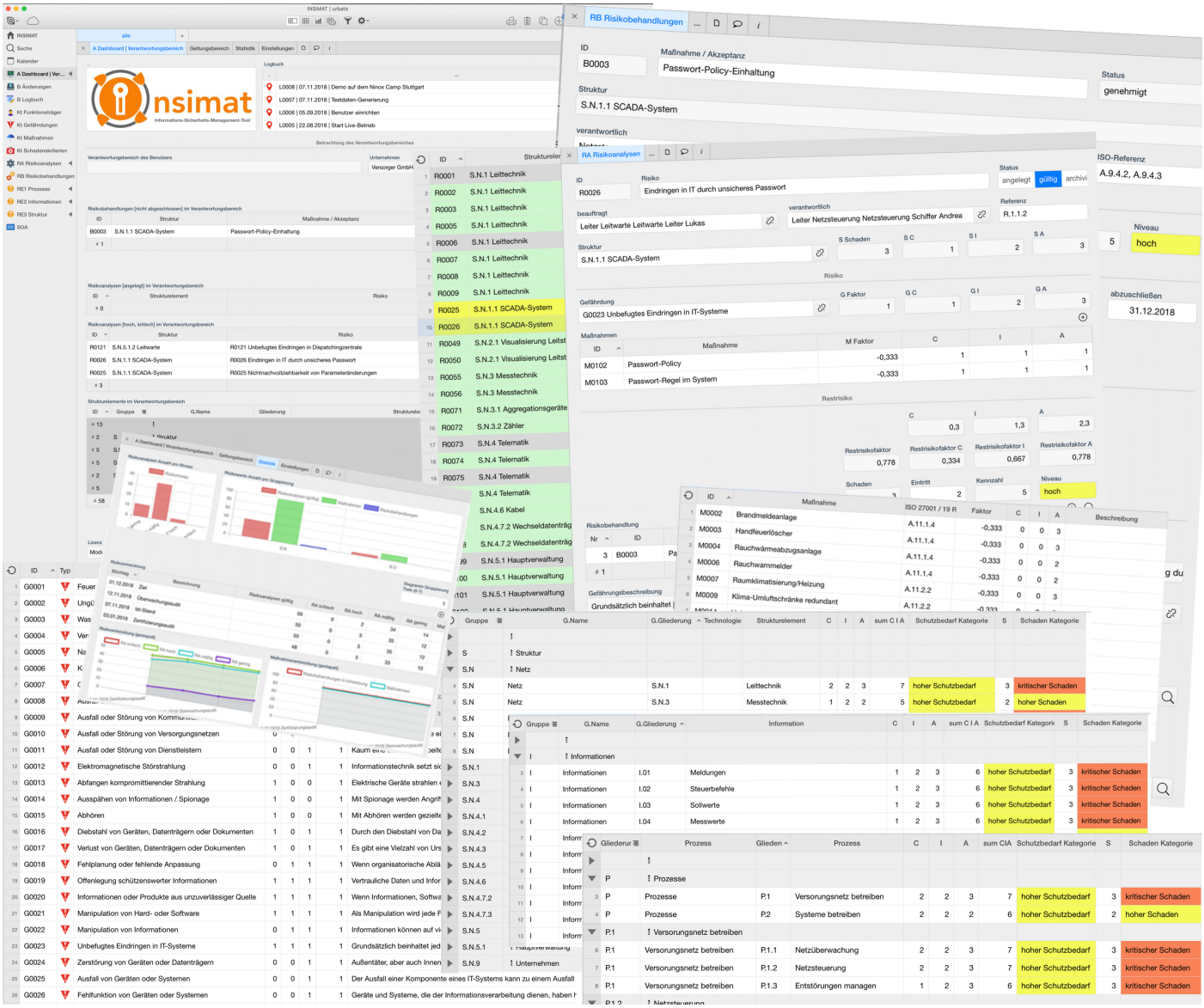
Backups werden von der Plattform auf dem Server automatisch durchgeführt und sollten darüberhinaus plattformunabhängig durch Server-Backups ergänzt werden.

Ein Benutzermanagement erlaubt die Administration der Plattform, der Anwendung und der Rollen und Berechtigungen der einzelnen Anwender und ermöglicht auch eine Trennung der Daten nach Anwendergruppen oder Unternehmen.

Leistungsmerkmale

	Hierarchische Abbildung der Prozess-, Informations- und Netz- & Organisations-Struktur mit individuellen Parametern		Dashboards und Auditberichte und tabellarische Sichten
	Vererbung des Schutzbedarfs und der Schadensauswirkung von Prozessen über Informationen zur Netz- und Organisations-Struktur		Ansichten, Filter- und Suchfunktionen
	Top-Down-Risikoanalyse von der groben Betrachtung iterativ in die Verfeinerungen		Rollen & Berechtigungen und Verantwortlichkeiten
	Automatische Kalkulation des Risikoniveaus und Restrisikos und manuelle Überschreibbarkeit der Kalkulationsparameter		CSV-Import und Export
	Eingabe über Formulare Ansicht und Überarbeitung in Tabellenform		Individuelle Anpassbarkeit der Algorithmen und Erweiterbarkeit der Datenstruktur
	Verwaltung von Dokumenten als Anhänge der Datensätze		Basierend auf LevelDB, einem performanten Key-Value Store Datenbankmodell
	PDCA (Plan-Do-Check-Act) Prozess Implementierung		Web-Front-End, iOS, MacOS und Android-App
	Logbuch und Änderungshistorie		Public Cloud / Private Cloud
	Nutzung von Bibliotheken • BSI-Gefährdungskataloge • ISO27001 Maßnahmenziele • Individuelle Risiken und Gefährdungen • weiteres KnowHow hinzufügbar		Weitere Module: • Workflowmanagement • Changemanagement • Assetmanagement • Datenschutzgrundverordnung (DSGVO) • Entwicklung individueller Module oder einer eigenen Plattform möglich
	Integration mit anderen Systemen über API		
	Kontinuierliche Weiterentwicklung und Ergänzung der Leistungsmerkmale		
	Support für Datenmigration, Installation, Konfiguration, Anpassungen und Schulung		
	Anwenderorientierte Preisgestaltung, abhängig von Unternehmensgröße / Anwendungsbereich und Anzahl der Benutzer		

Oberfläche



Rezensionen

„Nachdem wir unser ISMS als Prototyp in Excel realisiert hatten, haben wir uns entschlossen die entwickelten Datenstrukturen und Algorithmen in einer Datenbank-Anwendung mit Web-Front-End umsetzen zu lassen und alle Daten zu migrieren.
Der INSIMAT erfüllt alle unsere Anforderungen und bietet viel Potential für weitere Anwendungsfelder und Effizienzsteigerungen bei der Sicherstellung der Informations-Sicherheit in unserem Unternehmen.
Gerne empfehlen wir dieser Werkzeug weiter und laden Interessierte ein, im Rahmen eines Forums, die Effizienz dieses Werkzeugs zusammen mit uns weiter zu steigern.“
(Alexander Menges, Informations-Sicherheits-Beauftragter terranets bw)

„*Eine sehr strukturierte, übersichtliche und mustergültige Anwendung*" (Auditor des TÜV Rheinland)

„*Das beste was ich bisher gesehen habe*“ (Auditor des TÜV SÜD)

Weitere Informationen und Kontakt

Gerne beantworten wir Ihnen Ihre Fragen oder zeigen Ihnen den INSIMAT über eine WebEx.

urbato GmbH, IKT-Prozessberatung,
Horb am Neckar, www.urbato.de, info@urbato.de, +49 7451 622 99 59, +49 170 926 1828