GSTOOL QUO VADIS?

EVALUATION VON INFORMATION SECURITY MANAGEMENT SYSTEM TOOLS ALS GRUNDSCHUTZ TOOL ALTERNATIVEN

Cybersecurity Consulting Germany

VORWORT

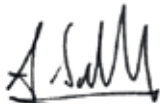
Bundestag, KFZ-Zulassungsbehörden in Hessen und Rheinland-Pfalz, Sony und TV-Monde. Hackangriffe sind an der Tagesordnung. Ein angemessenes Schutzniveau von IT-Systemen sicherzustellen ist daher von hoher Priorität.

Seit 1998 stellte das Bundesamt für Sicherheit in der Informationstechnik (BSI) erfolgreich eine Software für Anwender der BSI IT-Grundschutz Methodik bereit. Am 19. September gab das BSI jedoch bekannt, dass es das Grundschutz Tool (GSTOOL) aus wirtschaftlichen Gründen nicht weiterentwickelt wird. Jeglicher Support wird Ende 2016 eingestellt.

Für die Verantwortlichen in Bundesbehörden und andere Anwender des IT-Grundschutzes stellt sich daher nicht nur die Frage, welches Softwareprodukt sie in Zukunft bei Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten unterstützen soll, sondern auch, wie sie die bestehenden Daten migrieren sollen.

Unser Team von IT-Grundschutz und Informationssicherheitsexperten hat daher Softwareprodukte aus dem Informationssicherheitsmanagement (ISMS) von acht Herstellern als Alternative und Nachfolger des GSTOOL analysiert. Wir möchten uns an dieser Stelle für Ihre Teilnahme und konstruktive Zusammenarbeit bedanken.

Wir hoffen, dass wir Ihnen mit der Studie eine Entscheidungsgrundlage liefern können und sind an Ihrem Feedback interessiert. Wir freuen uns darauf, Sie bei Ihrer Migration zu einem neuen Grundschutz Tool oder Fragen der Informationssicherheit zu begleiten und zu unterstützen.



Dr. Alexander Schellong
General Manager
Cybersecurity Central & Eastern Europe,
Italy and Turkey

Peter Rehäusser
Head of Consulting
Cybersecurity Consulting Germany

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

MANAGEMENT SUMMARY

Am Markt sind eine Vielzahl von ISMS-Tools als Alternative zum GSTOOL vertreten. Für diese Studie wurden die Produkte von acht Herstellern analysiert. Zur besseren Vergleichbarkeit wurde das GSTOOL in der Version 4.8 ebenso in die Studie mit einbezogen. Hierfür mussten die Hersteller Fragenkataloge mit den wichtigsten Anforderungen beantworten. Diese wurden zusammen mit den Ergebnissen eines Anwendungstest ausgewählter Produkte durch ein Team von Grundschutz und Informationssicherheitsexperten ausgewertet.

Die Auswertung der Fragebögen ergab, dass Verinice (.PRO), HiScout GRC Suite, QSEC und iris sind in heterogenen und geografisch verteilten Umgebungen empfehlenswerte ISMS-Tools. Ihre Hardware- Anforderungen sind jedoch relativ hoch. Opus-i von kronsoft stellt eine weniger resourcenintensive Alternative dar. Bei diesem Produkt sind wie auch bei anderen Tools die IT-Grundschutz-Kataloge als HTML-Dateien, die das BSI bei jeder Ergänzungslieferung bereitstellt, hinterlegt. Die HiScout GRC Suite erfüllt diese Anforderung ebenfalls und kann zusätzlich durch die Unterstützung von ISMS- Managementprozessen und -Workflows überzeugen. Die Grundschutz-Kataloge sind auch hier standardmäßig hinterlegt, und der Nutzer hat die Möglichkeit die Kataloge – beispielsweise bei einer neuen Ergänzungslieferung – eigenständig zu importieren. Die Sicherheitsdatenbank SAVe ermöglicht ebenfalls seinen Nutzern ein ISMS gemäß IT-Grundschutz einzuführen, aufrechtzuerhalten bzw. fortzuschreiben. Außerdem punktet SAVe durch vielfältige Reportingfunktionen. Das Tool QSEC Suite ist – wie auch andere betrachtete Tools – eher eine Enterprise- Lösung mit sehr umfangreichem Spektrum an Einsatzmöglichkeiten einschließlich Governance-Risk-Compliance (GRC) und Information Security Management System (ISMS). Das Tool ist daher nur bedingt als Ersatz für das GSTOOL zu betrachten.

Die Anwendertest der ISMS-Tools von verinice und SAVe ergaben, dass sie sowohl in Bezug auf die Umsetzung der Anforderungen nach IT-Grundschutz als auch in Bezug auf die Handhabung bzw. Bedienung empfehlenswert sind. Informationsverbünde können schnell und einfach modelliert werden. Auch Schutzbedarfsfeststellungen oder Basis-Sicherheitschecks stellen keine große Hürde dar, sondern sind schnell intuitiv bedienbar.

Es wurde deutlich, dass die untersuchten ISMS-Tools in den Bewertungskategorien heterogene Stärken und Schwächen aufweisen. Eine eindeutige Empfehlung für ein Produkt ist daher nicht möglich. Die Ergebnisse erlauben GSTOOL Nutzern eher, ein für ihre Bedürfnisse geeignetes Produkt zu ermitteln. Die individuellen Anforderungen der Nutzer bestimmen, welche ISMS-Tools zum Einsatz kommen sollten.

1. EINLEITUNG UND ZIELSETZUNG

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat mit dem IT Grundschutz eine Methode für ein effektives Management der Informationssicherheit entwickelt. Sie lässt sich flexibel an die Gegebenheiten einer Organisation anpassen. Ebenso lassen sich Gefährdungen und Risiken ermitteln und Maßnahmen für den betroffenen Geltungsbereich (IT-Verbund) ableiten.

Mit dem Grundschutztool (GSTOOL) stellt das BSI eine Software bereit, die bei der Erstellung, Verwaltung und Fortschreibung von Sicherheitskonzepten gemäß IT-Grundschutz unterstützt. Das GSTOOL 4.8 wird jedoch nicht weiterentwickelt und auch der Support wird bis Ende 2016 komplett eingestellt. Neben dem offiziellen GSTOOL des BSI wurden von verschiedenen Herstellern ebenfalls Softwareprodukte entwickelt, welche die BSI-Standards umsetzen und welche das GSTOOL in Zukunft ablösen könnten.

Das Ziel dieser Untersuchung ist die vergleichende Analyse und anschließende Evaluation der am Markt befindlichen ISMS-Tools, die für die Implementierung und Fortschreibung von IT-Grundschutz vor allem bei Mittelständlern und Behörden geeignet sind und als Alternative für das GSTOOL in Frage kommen.

Die Untersuchung der ISMS-Tools erfolgt auf der Grundlage von ausgewählten Bewertungskriterien. Diese Kriterien repräsentieren Anforderungen von Nutzern, IT-Sicherheitsbeauftragten, Auditoren und erfahrenen Beratern an ein effizientes und effektives ISMS-Tool. Die Kriterien spiegeln somit elementare Anforderungen derjenigen wieder, die für die Implementierung, den Betrieb, die Weiterentwicklung und/ oder die Auditierung eines ISMS zuständig sind. Das übergeordnete Ziel dieser Studie ist, Tool-Empfehlungen zu geben, die die individuellen Anforderungen der unterschiedlichen Nutzer berücksichtigen und dadurch bedarfsgerechte Lösungen darstellen. Der ideale Nachfolger für das GSTOOL wird nicht identifizieren.

Zunächst wird eine Definition respektive Abgrenzung der Begriffe ISMS und ISMS-Tool vorgenommen. Anschließend werden der Aufbau bzw. die Durchführung der Studie beschrieben, ihre Ergebnisse vorgestellt und schließlich interpretiert. Im letzten Schritt werden auf Grundlage dieser Ergebnisse Empfehlungen formuliert.

[1] *Vgl. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/BSI_stellt_Entwicklung_GSTOOL_5_ein_19092013.html;jsessionid=E411CCFC382A1E812384BF8335A7AF02.2_cid286*

2. ISMS UND ISMS-TOOLS

In diesem Abschnitt wird eine begriffliche Abgrenzung zwischen ISMS und ISMS-Tool vorgenommen. Dabei stützt sich die Abgrenzung größtenteils auf Definitionen aus verschiedenen Normen (z.B. ISO 27001, IT-Grundschutz).

Was genau versteht man unter einem ISMS?
Ein Informations-Sicherheits-Management-System (ISMS) bewahrt unter der Anwendung von Risikomanagementprozessen die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und suggeriert damit nach außen, dass Risiken kontinuierlich identifiziert und adäquat behandelt werden (Definition gem. ISO 27001).

Gem. BSI Standard 100-1 werden unter einem Managementsystem generell aufeinander abgestimmte Regelungen zusammengefasst, die steuernde und lenkende Funktionen erfüllen und somit zur Erreichung von Geschäfts- bzw. Unternehmenszielen maßgeblich beitragen. Ein ISMS – also ein Managementsystem für Informationssicherheit – definiert, welche verschiedenen Methoden und Instrumente zur Steuerung und Lenkung der Aufgaben und Aktivitäten in Bezug auf Informationssicherheit von der Unternehmensleitung festgelegt werden. Dazu zählt Planung, Einsatz, Durchführung, Überwachung und Verbesserung dieser Methoden und Instrumente. Darüber hinaus können Managementsysteme kontinuierlich verbessert bzw. an neue Rahmenbedingungen angepasst werden.

Folgende Komponenten sind laut BSI Standard 100-1 grundlegende Bestandteile eines ISMS:

- Management-Prinzipien
- Mitarbeiter
- Ressourcen
- Sicherheitsprozesse:
    - Leitlinie zur Informationssicherheit (enthält definierte Sicherheitsziele und die Strategie zu ihrer Umsetzung)
    - Sicherheitskonzept
    - Informationssicherheitsorganisation

Die Umsetzung der in der Leitlinie zur Informationssicherheit enthaltenen / definierten Sicherheitsstrategie wird durch das Sicherheitskonzept und die Informationssicherheitsorganisation gewährleistet.

Was ist ein ISMS-Tool und wozu dient es?
Aufgrund zunehmender Komplexität in der IT-Landschaft sind die Implementierung, der Betrieb und die kontinuierliche Weiterentwicklung eines ISMS ohne Softwareunterstützung mittlerweile kaum noch denkbar. Es fallen dabei viele unterschiedliche Aufgaben an, die nicht immer ohne weiteres bewältigt werden können.

Datenerfassung bzw. -pflege, Modellierung von Informationsverbünden, Durchführung von Struktur-, Schutzbedarfs- und Risikoanalysen, Definition von Workflows, Zuordnung von Verantwortlichkeiten, Erstellung von Richtlinien, adäquate Dokumentation, Erstellung bzw. Überarbeitung von Sicherheitskonzepten, Definition, Durchführung und Nachverfolgung von Maßnahmen – kurz gesagt: alle Herausforderungen die mit der Implementierung, dem Betrieb und der kontinuierlichen Weiterentwicklung eines effektiven und effizienten ISMS einhergehen, können mit einem sogenannten ISMS-Tool erheblich vereinfacht und in den meisten Fällen standardkonform und revisionssicher abgebildet bzw. bewältigt werden.

3. STUDIE

Bereits nach ersten Recherchen wurde deutlich, dass eine Vielzahl unterschiedlicher ISMS-Tools am Markt vertreten ist. Diese Tools unterscheiden sich teilweise sehr stark voneinander. Dadurch erwies es sich anfänglich als äußerst schwierig eine gemeinsame Bewertungsgrundlage zu erarbeiten. Schließlich wurde gemeinsam mit Experten aus dem Informationssicherheitsumfeld ein Fragenkatalog definiert, der alle relevanten Bewertungskriterien eines effektiv und effizient arbeitenden ISMS-Tools abdeckt. Es muss jedoch darauf hingewiesen werden, dass es sich bei manchen der untersuchten Produkte nicht nur um reine ISMS-Tools zur Abbildung des IT-Grundschutzes handelt, sondern um Softwareprodukte zur Unterstützung des umfassenderen Governance, Risk & Compliance (GRC) Managements (s. **TABELLE 1** in Kapitel 5).

Bewertet bzw. getestet wurden ausschließlich Eigenschaften der Tools im Hinblick auf die Entwicklung bzw. Aufrechterhaltung eines ISMS gemäß IT-Grundschutz des BSI. Aus diesem Grund werden die Softwareprodukte der Hersteller alle unter dem Begriff „ISMS-Tool“ zusammengefasst – auch wenn sie mehr Eigenschaften inne tragen

3.1 Fragenkatalog

Zur Bewertung der unterschiedlichen Tools wurde gemeinsam mit erfahrenen Experten aus dem IT-Grundschutzumfeld ein Fragenkatalog entwickelt, der die Anforderungen an ein effektives ISMS-Tool anhand verschiedener Kriterien widerspiegelt. Dieser Fragenkatalog wurde an die Hersteller von ISMS-Tools verschickt. Die von den Produktherstellern ausgefüllten Fragenkataloge wurden ausgewertet, indem die Informationen bzw. Angaben seitens der Hersteller über die einzelnen Produkte zunächst konsolidiert und anschließend evaluiert wurden.

Folgende Tools wurden im Zuge dieses Vergleichs in ihrer aktuellen Version näher betrachtet:

- DHC Vision Information Security Manager 5.2
- GSTOOL V4.8
- HiScout GRC Suite 2.3
- iris (Version 15/R2 (Build 15107.1))
- Opus-i (Oktober 2014)
- QSEC V4.2
- SAVe V4.4 bzw. V5.0
- Sidoc (Oktober 2014)
- Verinice 1.9.

Bei den untersuchten Produkten handelt es sich größtenteils um Tools, die durch das BSI lizensiert wurden. Eine Lizensierung durch das BSI bestätigt, dass ISMS-Tools in der Lage sind, den IT-Grundschutz umzusetzen bzw. bei seiner Umsetzung zu unterstützen. Diese Vorauswahl soll andere Tools nicht diskriminieren sondern war lediglich ein pragmatischer Ansatz, den Umfang dieser Studie zu definieren. Weitere Produkthersteller wurden angefragt, wollten sich allerdings nicht an dieser Studie beteiligen. Außerdem stellen alle betrachteten Produkte Experten-Tools dar, die Kenntnisse in der Grundschutz-Methodik voraussetzen.

Bevor die einzelnen ISMS-Tools analysiert werden können, mussten adäquate Anforderungen definiert werden. Diese Anforderungen spiegeln die folgenden Bewertungskriterien bzw. –kategorien wider:

- Systemvoraussetzungen
- Umsetzung der BSI IT-Grundschutz Standards (100-x)
- Umsetzung ISO 27001
- Risikoanalyse
- ISMS Managementprozesse & Workflows
- Reporting
- Benutzbarkeit (Usability).

Im Fragenkatalog, der den Herstellern zugesandt wurde, wurden die Produkteigenschaften der einzelnen Tools im Zusammenhang mit den o. g. Kriterien durch entsprechende Fragen adressiert.

Bei der Bewertung der Tools diente folgende Skalierung als Grundlage:

1. Nicht anwendbar
2. Sehr Hoch
3. Hoch
4. Mittel
5. Niedrig

bzw.

1. Nicht anwendbar
2. Nicht vorhanden / nicht akzeptabel
3. Teilweise vorhanden / erfüllt
4. Gut
5. Sehr gut.

Die erste Skalierung wurde ausschließlich bei der Bewertung der Systemvoraussetzungen verwendet. Bei den Bewertungen in Bezug auf Systemvoraussetzungen bedeuten hohe Bewertungen, dass die entsprechenden Tools aus unserer Sicht geringfügige Anforderungen beispielweise an die Hardware stellen bzw. viele verschiedene Datenbanken unterstützt. Bei allen in den Abbildungen dargestellten Ergebnissen gilt: Je höher die Bewertung/ Ausprägung desto besser.

Die Bewertungskriterien wurden von Experten ebenfalls gewichtet. Der Gewichtung liegt dabei folgende Skalierung zugrunde:

- 1: kann entfallen
- 2: „nice to have“
- 8: sollte möglich sein
- 20: muss möglich sein.

Die Angaben aus den ausgefüllten Fragenkatalogen der einzelnen Produkthersteller wurden konsolidiert, bewertet und gegenübergestellt.

3.2 Ergebnisse

Es wird nochmals darauf hingewiesen. dass diese Studie nicht das Ziel verfolgt, das „beste“ ISMS-Tool zu identifizieren. Eher soll es die Stärken der einzelnen Tools in den Vordergrund stellen und einen Überblick über die verschiedenen Produkteigenschaften, die unsere Experten im Zusammenhang mit dem IT-Grundschutz des BSI als relevant erachten, verschaffen.

Die folgende **ABBILDUNG 1** zeigt die zusammengefassten Studienergebnisse und verdeutlicht, dass sich die untersuchten ISMS-Tools in einigen Bewertungspunkten stark, in anderen wiederum nur geringfügig voneinander unterscheiden.

In der Bewertungskategorie „Risikoanalysen“ haben alle Tools die von unseren Experten als „Best Case“ definierte Höchstbewertung erreicht. Beim „IT-Grundschutz“ als Bewertungspunkt sind geringfügige Unterschiede zu erkennen. In den Bewertungskategorien „ISMS Managementprozesse“, „Reporting“, „Benutzbarkeit“, „Systemvoraussetzungen“ und „ISO 27001“ hingegen sind die Unterschiede zwischen den ISMS-Tools teilweise größer. Opus-i hat u.a. mit seinen niedrigen Hardwareanforderungen die bestmögliche Bewertung in der Kategorie „Systemvoraussetzungen“ erreicht, wohingegen DHC vergleichsweise hohe Anforderungen an die Hardware stellt

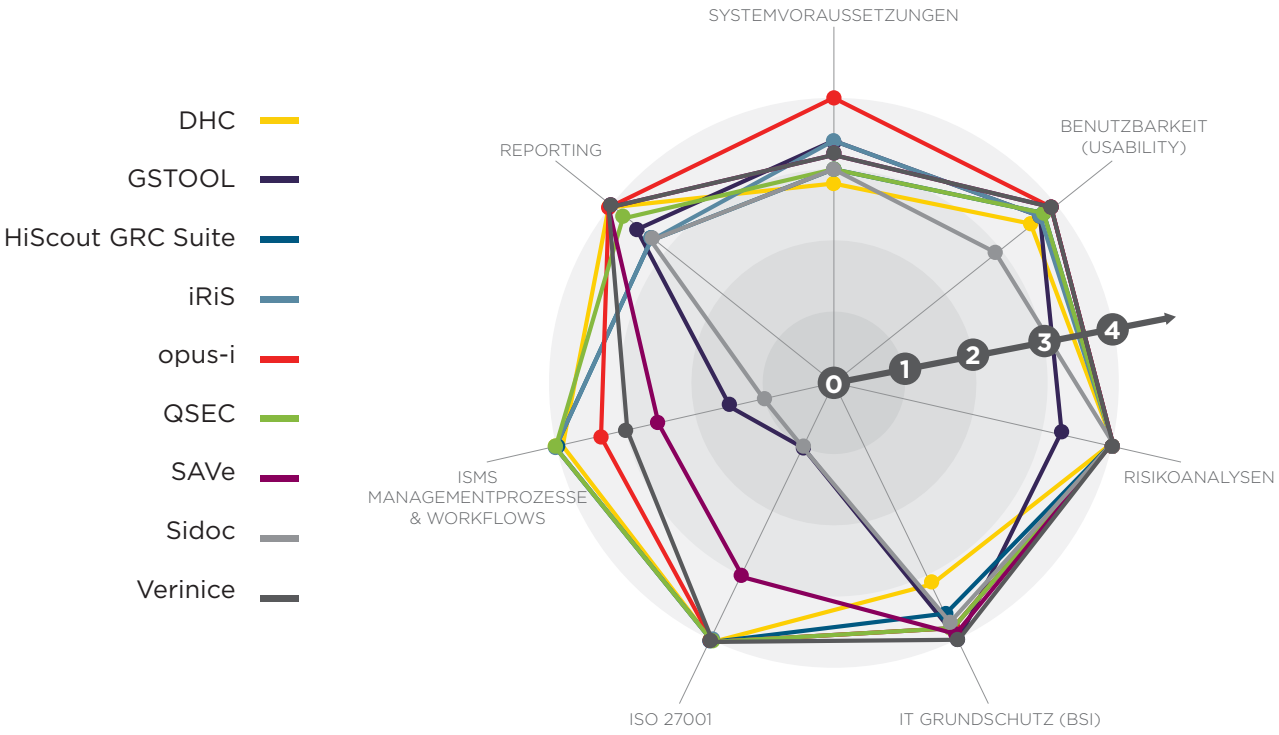
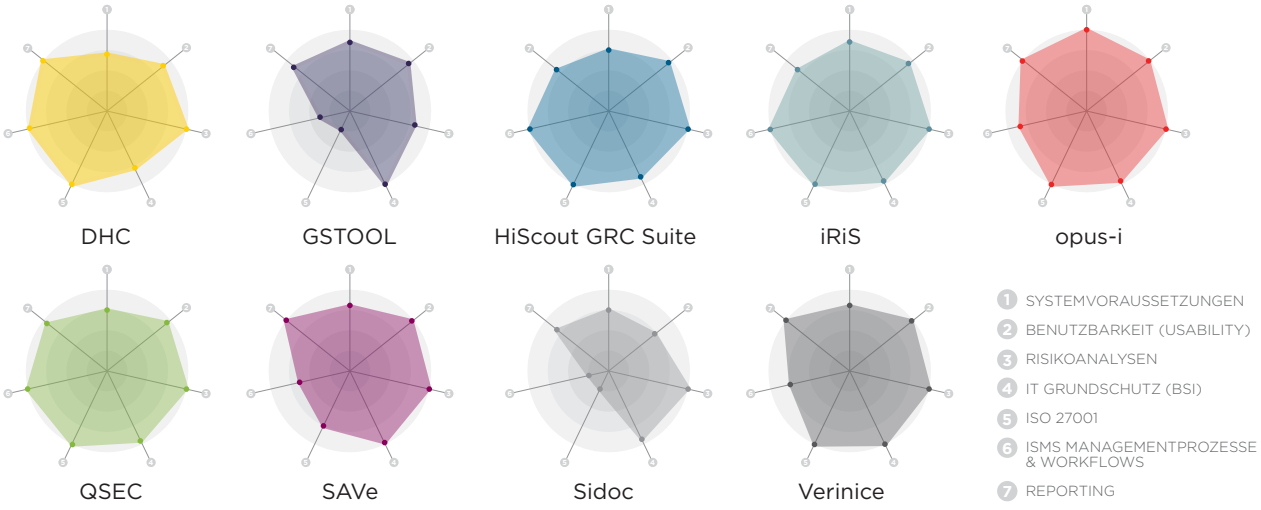


ABBILDUNG 1: ZUSAMMENFASSUNG DER STUDIENERGEBNISSE

Die Detailergebnisse pro Kategorie werden in den folgenden Abschnitten erläutert.



3.2.1 Systemvoraussetzungen

In der folgenden **ABBILDUNG 2** sind die Teilergebnisse zur Bewertungskategorie „Systemvoraussetzungen“ dargestellt. Die GRC Suite von HiScout, iris sowie QSEC überzeugen in dieser Gegenüberstellung durch die bestmöglichen Bewertungen hinsichtlich unterstützter Betriebssysteme sowie Hardwareanforderungen in Bezug auf Clients.

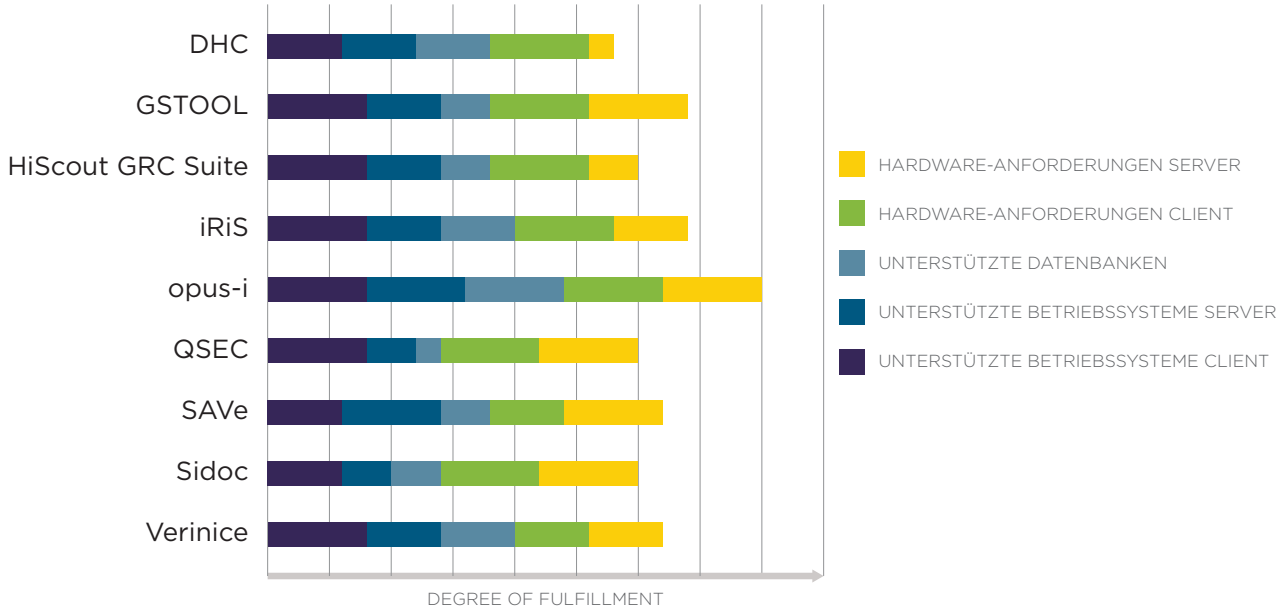


ABBILDUNG 2: TEILERGEBNISSE IM BEREICH SYSTEMVORAUSSETZUNGEN

3.2.2 IT-Grundschutz

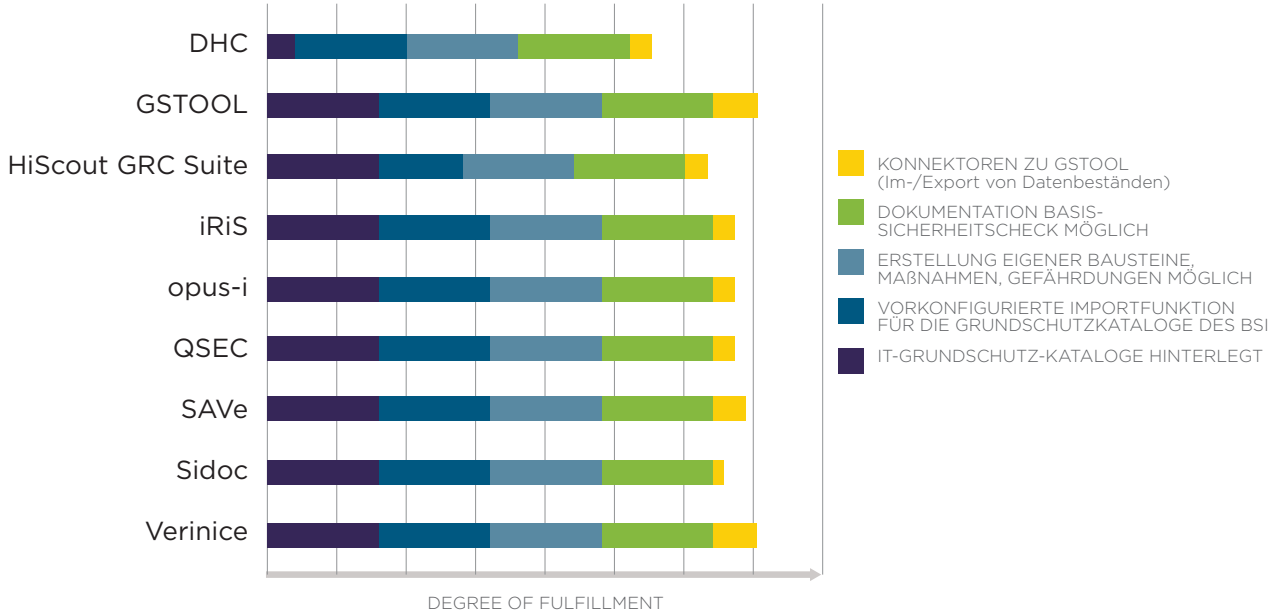


ABBILDUNG 3: TEILERGEBNISSE IM BEREICH IT-GRUNDSCHUTZ

Im Hinblick auf die Bewertungskategorie „IT-Grundschutz“ (ABBILDUNG 3) haben alle Tools eine identische Bewertung hinsichtlich der Dokumentation des Basis-Sicherheitschecks erreicht. In Bezug auf Konnektoren zum GSTOOL (für einen Im- bzw. Export von Datenbeständen) wurden auf Grundlage der Herstellerangaben teilweise größere Unterschiede festgestellt. Sidoc beispielsweise bietet in seiner aktuellen Version keine Konnektoren zum GSTOOL vom BSI[1] kommt, gibt es viele geeignete Alternativen auf dem Markt.

3.2.3 ISMS-Managementprozesse

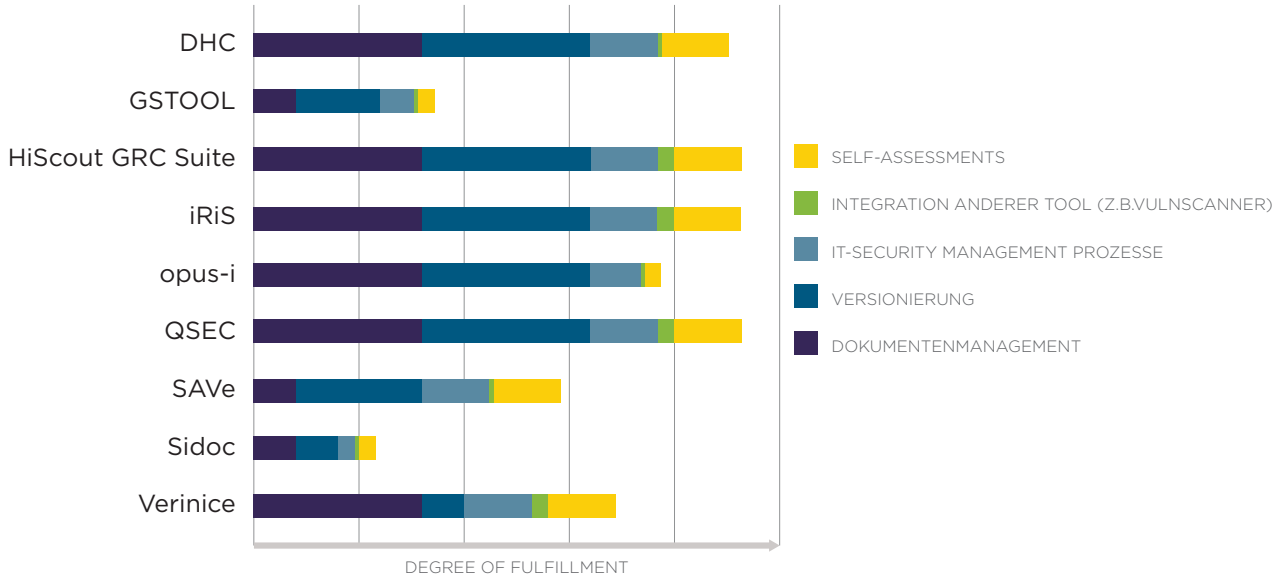


ABBILDUNG 4: TEILERGEBNISSE IM BEREICH ISMS MANAGEMENTPROZESSE

Hinsichtlich „Self-Assessments“, „Dokumentenmanagement“ und „Versionierung“ unterscheiden sich die untersuchten Tools teilweise sehr stark voneinander (s. **ABBILDUNG 4**) In Bezug auf „IT-Security Management Prozesse“ hingegen hat sich gezeigt, dass bei nahezu allen untersuchten ISMS-Tools vergleichbare bzw. ähnliche Produkteigenschaften vorhanden sind und die Anforderungen in diesen Bewertungskategorien größtenteils erfüllt werden. Die Integration weiterer Tools (z.B. Vulnerability Scanner) wird nur von wenigen der untersuchten ISMS-Tools unterstützt. Zu diesen ISMS-Tools gehören HiScout GRC Suite (via XML-Schnittstelle), iris (per Customizing) und verinice (Greenbone VulnScan).

3.2.4 Benutzbarkeit (Usability)

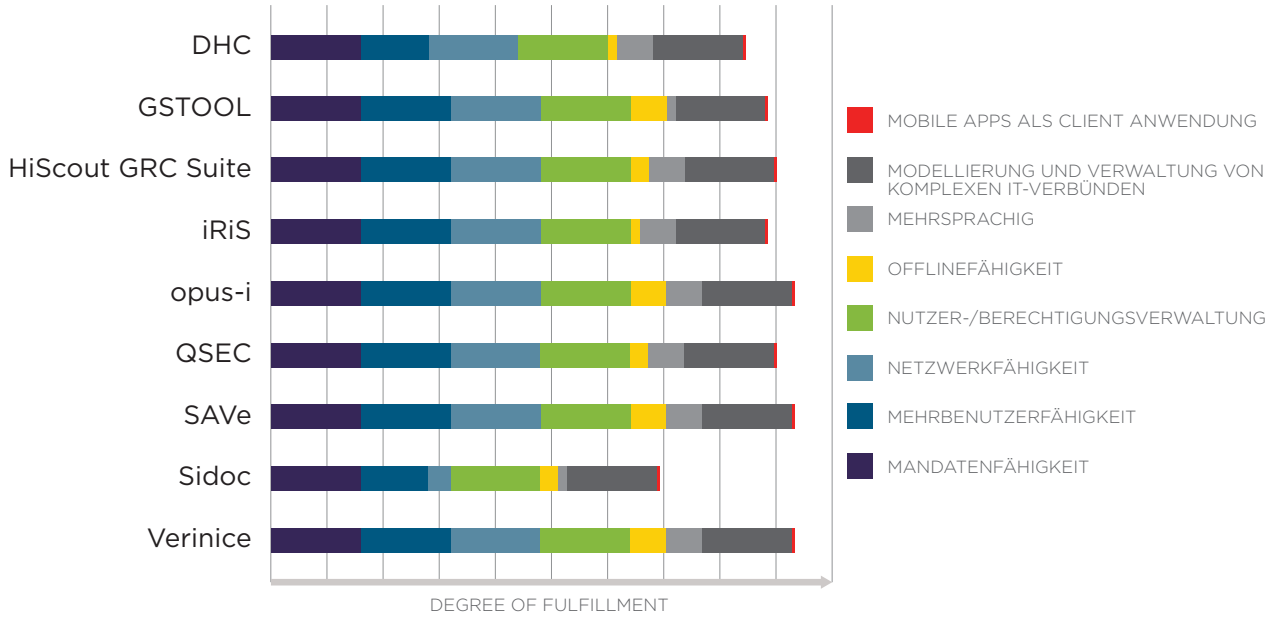


ABBILDUNG 5: TEILERGEBNISSE IM BEREICH BENUTZBARKEIT (USABILITY)

ABBILDUNG 5 zeigt die Detailergebnisse in der Bewertungskategorie „Benutzbarkeit“. Mobile Apps als Client Anwendungen werden ebenfalls von keinem der Tools angeboten. DHC plant nach eigenen Angaben die Entwicklung einer solchen App mit voraussichtlicher Fertigstellung bis Ende 2015. Die ISMS-Tools iris, DHC und QSEC bieten den

Nutzern nicht die Möglichkeit offline zu arbeiten. Eine bestehende Internetverbindung ist zwingend notwendig. Einmal online, steht dem Prozesseigentümer oder dem IT-Administrator in QSEC im Anwendermodus („Normal User“) eine übersichtliche GUI mit umfangreichen Funktionen zur Verfügung

ABBILDUNG 6: QSEC® STARTBILDSCHIRM (GUI)

QSEC eignet sich – wie auch die anderen betrachteten Tools – u. a. zum Erfassen der Zielobjekte (Assets) und ermöglicht einen strukturierten Überblick über die erfassten Asset(-gruppen) und alle zugehörigen relevanten Informationen.

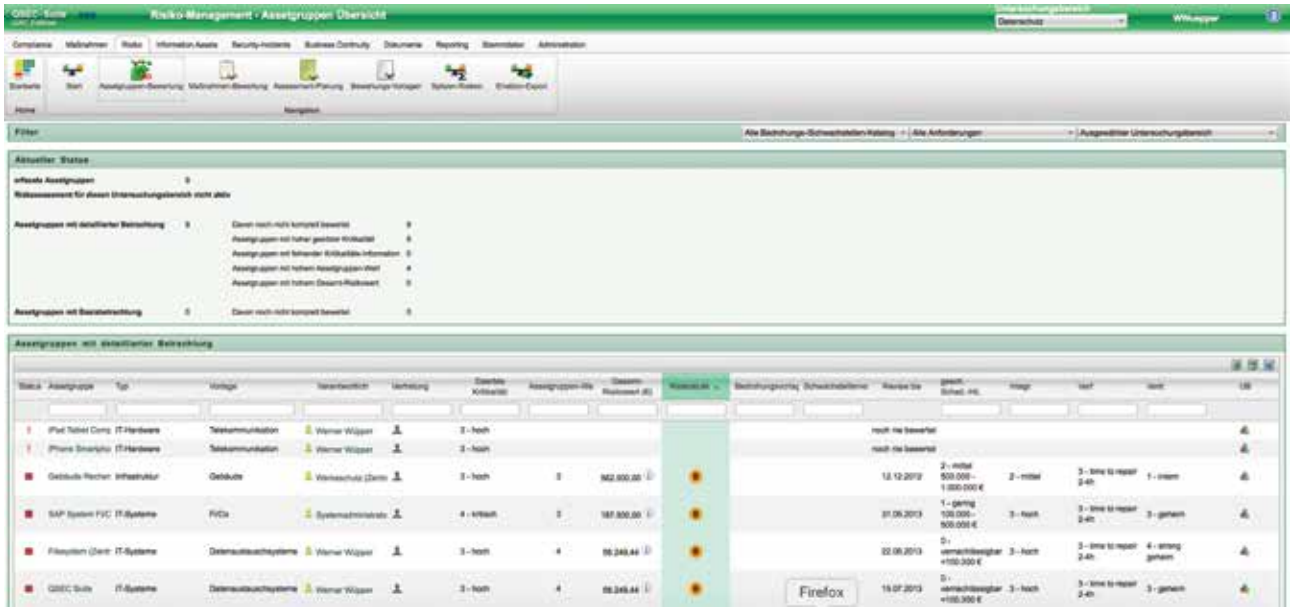


ABBILDUNG 7: ASSETGRUPPEN ÜBERSICHT in QSEC® (ANWENDERMODUS)

Auch iris gehört zu den Tools, die eine bestehende Internetverbindung benötigen (Web-Front-End). Das Dashboard macht einen übersichtlichen Eindruck und beinhaltet alle wichtigen bzw. offenen Aufgaben. Auf Wunsch (per Klick) des Anwenders werden nur die Daten in dessen Verantwortlichkeit angezeigt (s. **ABBILDUNG 8**).

[2] *Laut Herstellerangaben ist die Fertigstellung einer komplett neu entwickelten Nachfolgversion von Sidoc für 2015 geplant.*

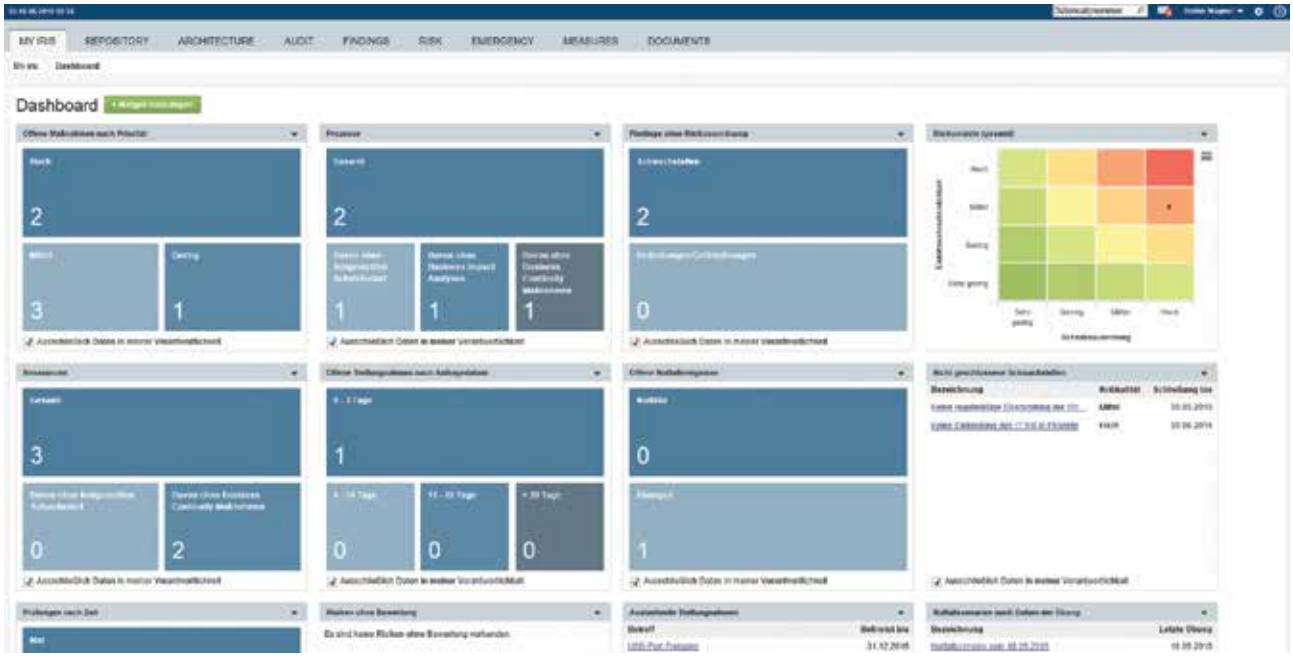


ABBILDUNG 8: iris® DASHBOARD

Die erfassten Geschäftsprozesse verfügen über verschiedene Reiter (z.B. Prozess- bzw. Ressourcenzuordnung, Schutzbedarf, Business Impact Analyse, Business Continuity Management, Handlungsempfehlungen, Dokumente usw.) und erleichtern damit ein systematisches Arbeiten. Schritt für Schritt werden alle relevanten Daten erfasst.

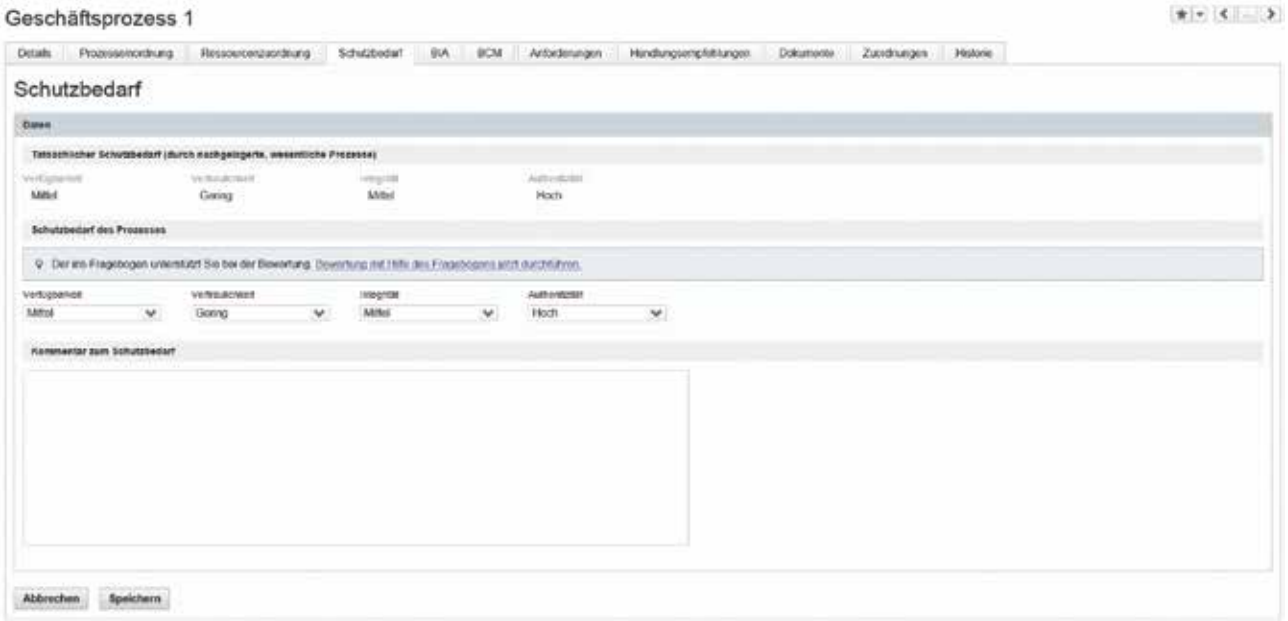


ABBILDUNG 9: SCHUTZBEDARFSFESTSTELLUNG IN iris®

Sidoc ist in seiner momentan verfügbaren Version nicht netzwerkfähig. Die Nutzer- bzw. Berechtigungsverwaltung, die Modellierung und Verwaltung von komplexen IT-Verbünden sowie die Mehrbenutzerfähigkeit werden von allen untersuchten ISMS-Tools unterstützt. Auch bei mehrsprachigen Tools ist Deutsch als Standardeinstellung vorinstalliert.

3.2.5 Risikoanalysen

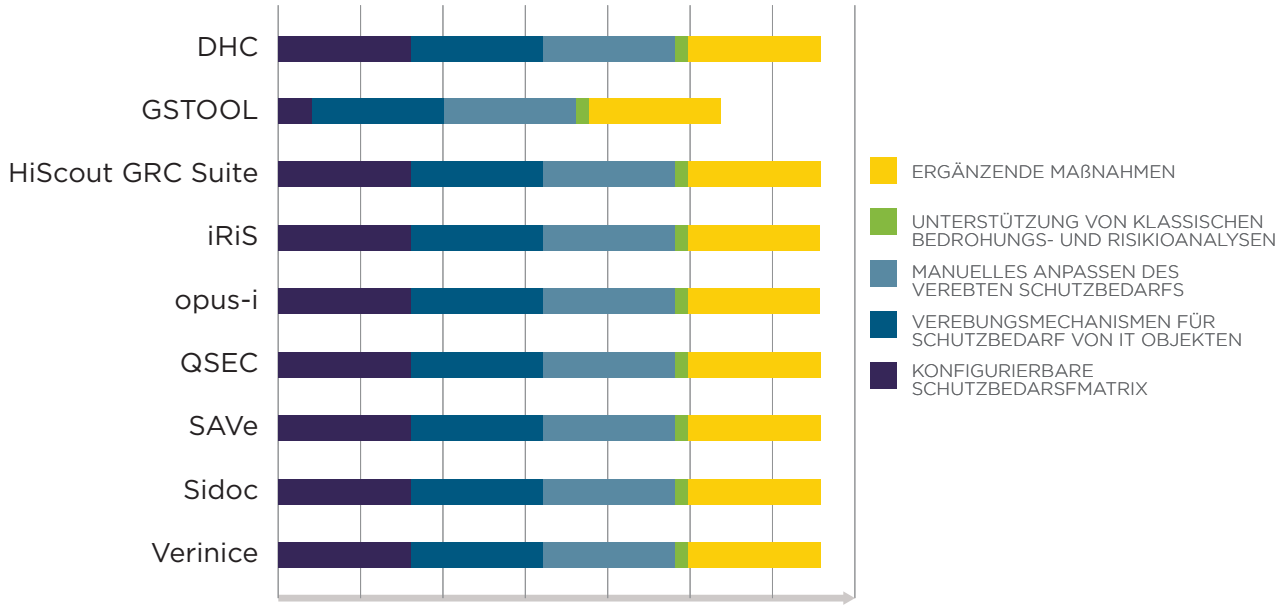


ABBILDUNG 10: TEILERGEBNISSE IM BEREICH RISIKOANALYSEN

Die in **ABBILDUNG 10** dargestellten Teilergebnisse in der Bewertungskategorie „Risikoanalysen“ zeigen deutlich, dass alle untersuchten Tools die Kriterien bzw. Anforderungen in dieser Kategorie erfüllen. Das GSTOOL ermöglicht es nicht die Schutzbedarfsmatrix zu konfigurieren, da es vom BSI-Standard nicht gefordert ist.

3.2.6 ISO 27001

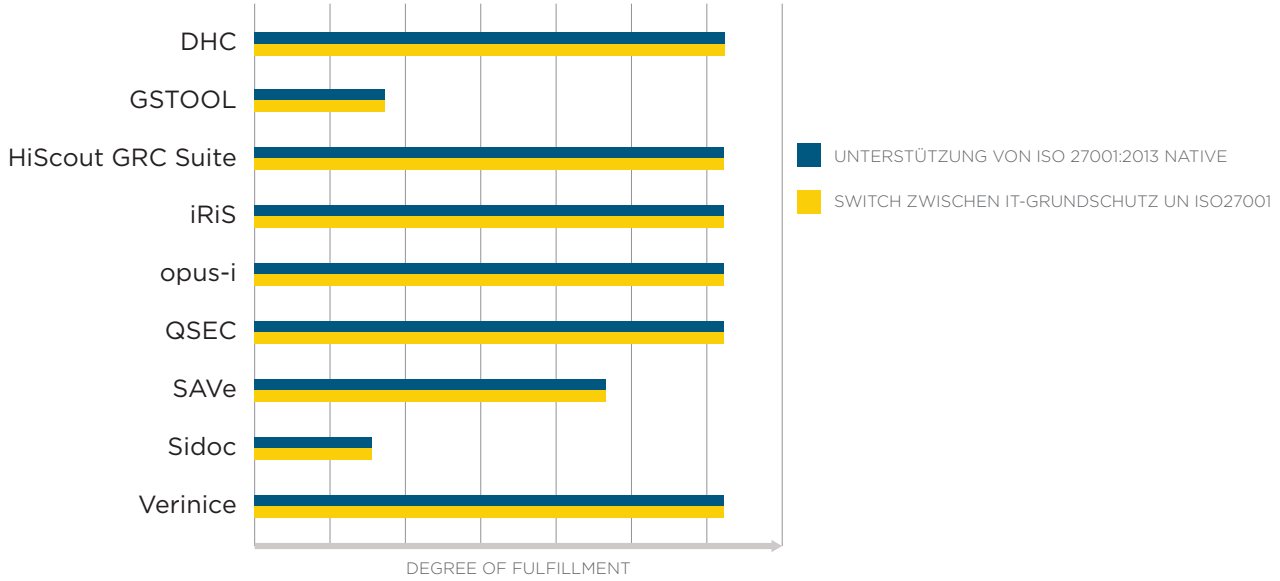


ABBILDUNG 11: TEILERGEBNISSE IM BEREICH ISO 27001

Die Detailergebnisse im Bereich ISO 27001 (s. **ABBILDUNG 11**) verdeutlichen, dass alle untersuchten ISMS-Tools bis auf Sidoc und das GSTOOL den ISO 27001-Standard unterstützen oder einen Switch zwischen IT-Grundschutz und ISO 27001 erlauben. Die IT-Sicherheitsdatenbank SAVe unterstützt zwar auch den ISO-Standard, bisher allerdings nur ISO 27001:2005.

3.2.7 Reporting

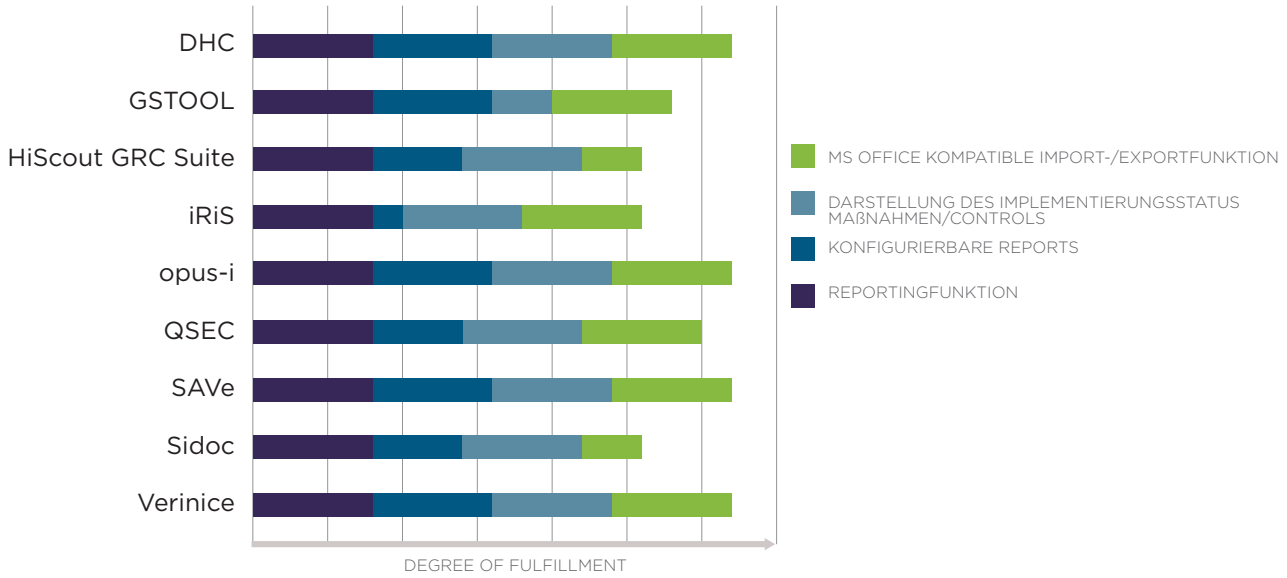


ABBILDUNG 12: TEILERGEBNISSE IM BEREICH REPORTING

Alle untersuchten Tools verfügen – wie in **ABBILDUNG 12** zu erkennen ist – über Reportingfunktionen und sind in der Lage den Implementierungsstatus der Maßnahmen darzustellen bzw. auszuwerten. Wenn eine Zertifizierung angestrebt wird, sind diese beiden Produkteigenschaften von großem Nutzen. Das GSTOOL richtet sich ausschließlich nach den (Zertifizierungs-)Vorgaben des BSI, weshalb die Darstellung des Implementierungsstatus der ISO 27001-Controls nicht notwendig bzw. nicht möglich ist. Bis auf QSEC und Sidoc bieten alle untersuchten Tools den Nutzern die Möglichkeit Berichte individuell zu konfigurieren und dem jeweiligen Bedarf anzupassen.

4. PRODUKTTESTS

Nach der Evaluierung der Tools auf Basis der von den Herstellern ausgefüllten Fragenkataloge wurden zwei Tools in Form von Produkttests näher betrachtet. Hierfür wurden im Vorfeld Testfälle definiert. Als Grundlage diente die Beispieldatenbank des BSI (BSIDB_V45), welche bei Installation des GSTOOLs bereitgestellt bzw. mitgeliefert wird. Hierbei handelt es sich um einen fiktiven Informationsverbund mit folgenden Eckdaten:

- eine Anwendung (Datenbank-Zugriffe)
- ein Gebäude, darin enthalten 2 Gruppen von Räumen (Gruppierung von Büroräumen und Server-Raum)
- ein heterogenes Netz (LAN)
- ein LAN-Switch
- ein Windows-basierter Server
- eine Gruppierung von Windows-Clients
- keine Netzübergänge zu anderen Systemen

Der Schutzbedarf ist durchgängig „normal“, da keine personenbezogenen Daten verarbeitet werden. Dieser beispielhafte Informationsverbund könnte ggf. zertifiziert werden und stellt somit die geeignete Grundlage für die Produkttests dar.

Neben der Abbildung bzw. Modellierung des beschriebenen Informationsverbunds gehören die Durchführung des Basis-Sicherheitschecks, die Installation/Konfiguration der Tools, das eigenständige Importieren von BSI IT-Grundschutz-Katalogen und Datenbanken aus dem GSTOOL 4.8 sowie die generelle Handhabung zu den Testfällen, die im Zuge dieser Produkttests durchlaufen werden. Es wurde bewusst ein Tester mit wenig Erfahrung im Umgang mit den betrachteten ISMS-Tools – mit Ausnahme des GSTOOLs – für die Produkttests ausgewählt, um möglichst objektive Ergebnisse auf Anfängerniveau zu erhalten.

Bei den getesteten ISMS-Tools handelt es sich um verinice V1.9 und eine Testversion der IT-Sicherheitsdatenbank SAVe. V4.4. Diese beiden Tools wurden für eine nähere Betrachtung ausgewählt, da sie zum einen neben weiteren

Tools den Anforderungen in der Bewertungskategorie „IT-Grundschutz“ mehr als gerecht werden und sich zum anderen insbesondere hinsichtlich der Bewertung in den Kategorien „ISMS Managementprozesse und Workflows“ und „ISO 27001“ voneinander unterscheiden. Diese Auswahl spiegelt jedoch keine grundsätzliche Entscheidung wider, nach der diese beiden Tools von den untersuchten die am besten geeigneten Alternativen für das GSTOOL sein sollen.

4.1 Verinice

Das von der SerNet GmbH entwickelte ISMS-Tool „verinice“ ist nicht nur als OpenSource-Version für den Client kostenlos downloadbar und stellt somit gerade für Einsteiger eine geeignete Übungsplattform dar, sondern hat in vielen Bewertungskategorien hohe Punktzahlen erreicht, was eine nähere Betrachtung des Tools rechtfertigt.

Die Installation der Software wie auch der Import der Grundschutzkataloge (14. Ergänzungslieferung) stellt selbst für Anfänger unter Verwendung von Anleitungen (u.a. im Support-Forum von SerNet) keine große Hürde dar. Nach ersten grundlegenden Konfigurationseinstellungen (z.B. Sprache, BSI IT-Grundschutz Perspektive) konnte mit dem Erfassen der Stammdaten bzw. Zielobjekte direkt begonnen werden. Als besonders hilfreich erwiesen sich die Tutorials in Form von „Spickzetteln“, die Schritt für Schritt Anweisungen bei grundlegenden Operationen bieten. Dadurch sollten selbst Anfänger in der Lage sein mit dem Tool umzugehen.

Beim Anlegen des Informationsverbunds (Schicht 1) kann man gleich zu Beginn die Schutzbedarfs-kategorien im Zielobjekte-Browser definieren bzw. anpassen. Besonders hervorzuheben ist die einfache Verknüpfung von Zielobjekten mittels „Drag & Drop“ und die automatische Vererbung des Schutzbedarfs, den man ggf. problemlos manuell anpassen kann.

Die Modellierung wird nach ein wenig Übung immer routinierter. Mehrere Bausteine können auf einmal zugeordnet werden, was den Aufwand bei der Modellierung erheblich reduziert.

Nach vollständiger Modellierung und Bearbeitung der entsprechenden Maßnahmen ist der Basis-Sicher-heitscheck mit wenigen Klicks durchgeführt.

ABBILDUNG 13 zeigt den in verinice modellierten Beispielverbund des BSI, wie er in der IT-Grundschutz-Perspektive dargestellt wird.

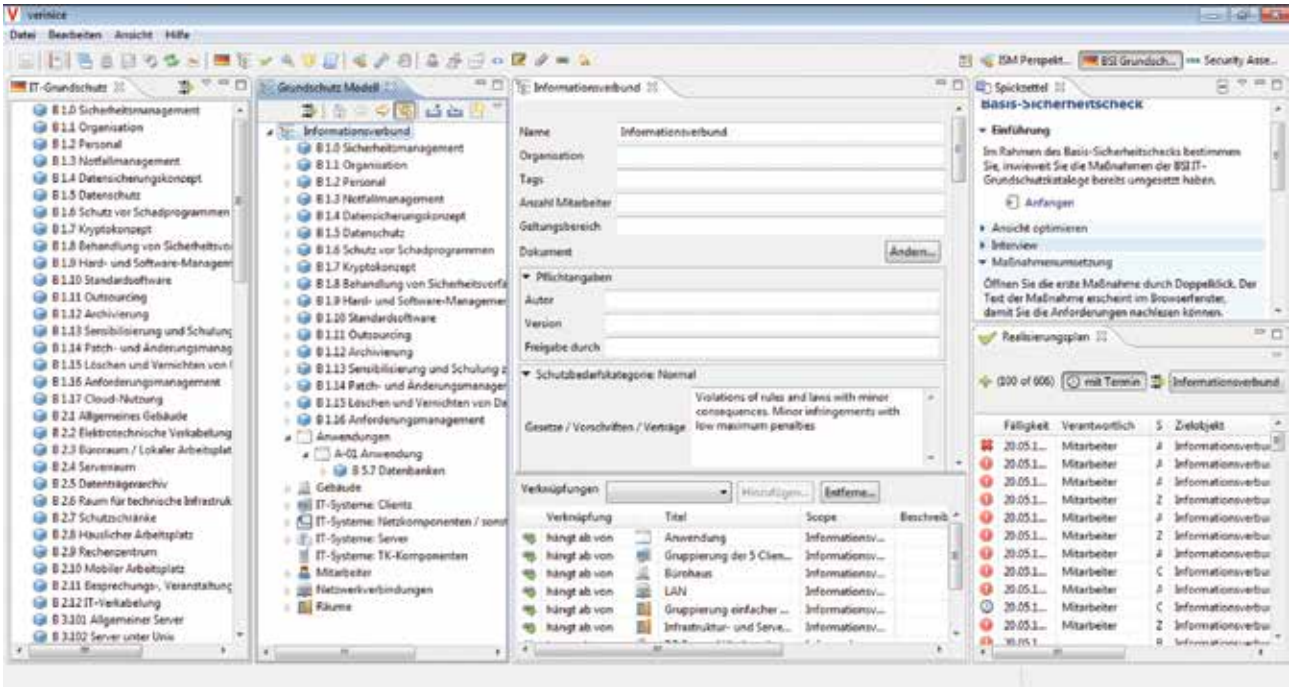


ABBILDUNG 13: MODELLIERUNG DES BEISPIELVERBUNDS IN VERINICE®

Zum Vergleich zeigt **ABBILDUNG 14** wie der Beispielverbund in der aktuellen Version (4.8) des GSTOOLs in der Zielobjekte-Ansicht angezeigt wird. An dieser Stelle fällt u.a. der große Unterschied bei der hierarchischen Anordnung der Zielobjekte besonders auf. Im GSTOOL folgt die Anordnung dem BSI Schichtenmodell (1 bis 5), was sich bei der Modellierung als vorteilhaft erweist. Bei verinice hingegen stehen die Räume an unterster Stelle im Informationsverbund, obwohl sie gem. BSI Schichtenmodell zu Zielobjekten der Schicht 2 (Infrastruktur) zählen.

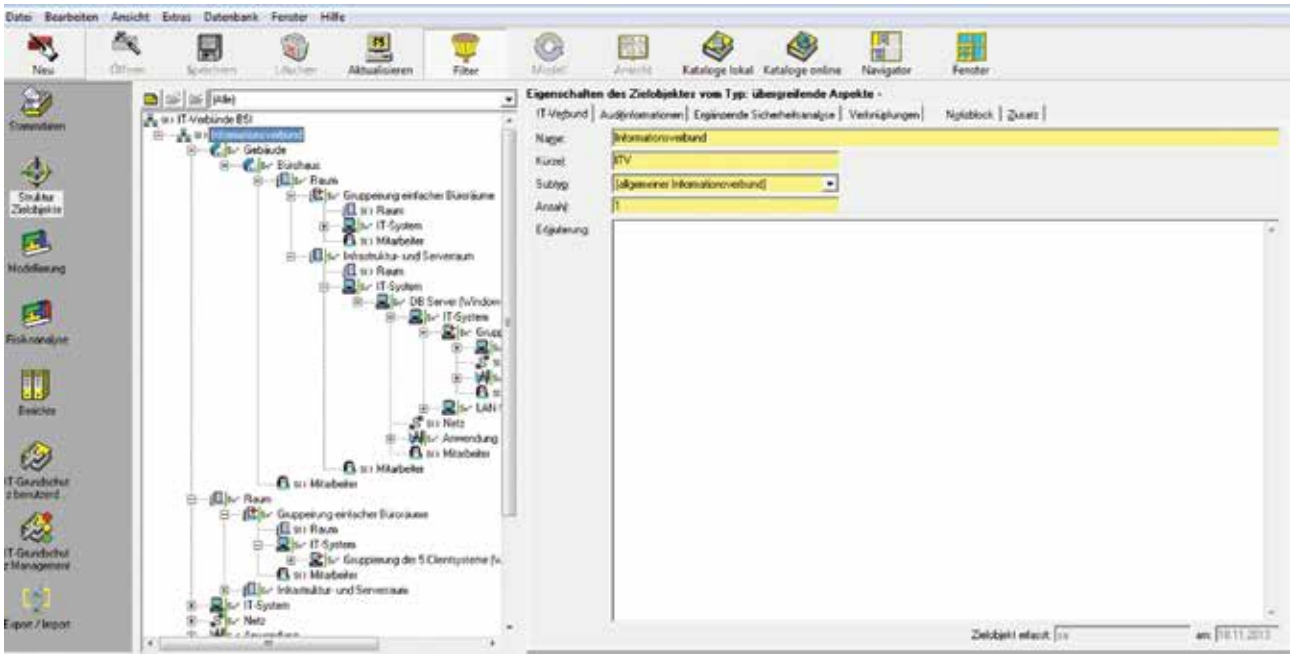


ABBILDUNG 14: BEISPIELVERBUND IN DER ZIELOBJEKTE-ANSICHT DES GSTOOLs 4.8

Auch das Importieren von Datenbeständen aus dem GSTOOL 4.8 stellt keine große Herausforderung für verinice dar. Nach wenigen Einstellungen können Informationsverbünde komplett und problemlos aus dem GSTOOL importiert werden (s. **ABBILDUNG 15**). Es kann jedoch dazu kommen, dass manche Zielobjekte im Zuge des Imports einer anderen Schicht bzw. Zielobjektekategorie zugeordnet werden. Daher ist es ratsam nach dem Import die Stammdaten und Verknüpfungen nochmals zu prüfen.

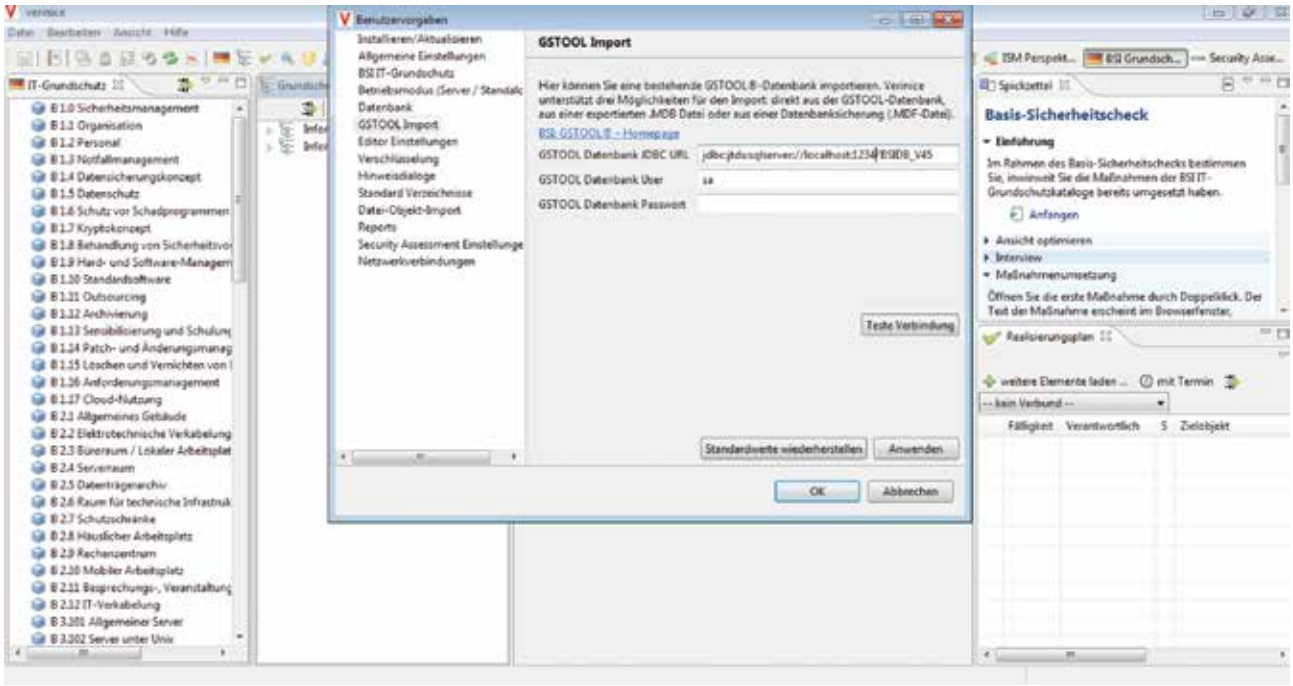


ABBILDUNG 15: GSTOOL IMPORT IN VERINICE®

4.2 SAVe

Das zweite Tool in unseren Produkttests ist die von der INFODAS GmbH entwickelte, auf Microsoft Access basierende IT-Sicherheitsdatenbank SAVe V4.4. Die Installation des Tools ist schnell durchgeführt – sofern man im Besitz einer gültigen Microsoft Access Lizenz ist. Das mitgelieferte bzw. auch online zur Verfügung gestellte, ca. 200 Seiten starke Benutzerhandbuch erwies sich insbesondere für Anfänger als sehr hilfreich. In der IT-Sicherheitsdatenbank selbst ist ein Assistent integriert, der bei der Erstellung eines Informationsverbunds / Daten-Modells Hilfestellungen bietet. Die GUI verdeutlicht im Gegensatz zu verinice die Anlehnung an das Microsoft-Design. Lediglich die Menüleiste auf der linken Seite (s. **ABBILDUNG 16**) könnte einem Anwender, der bisher nur mit dem GSTOOL des BSI gearbeitet hat, vertraut vorkommen.

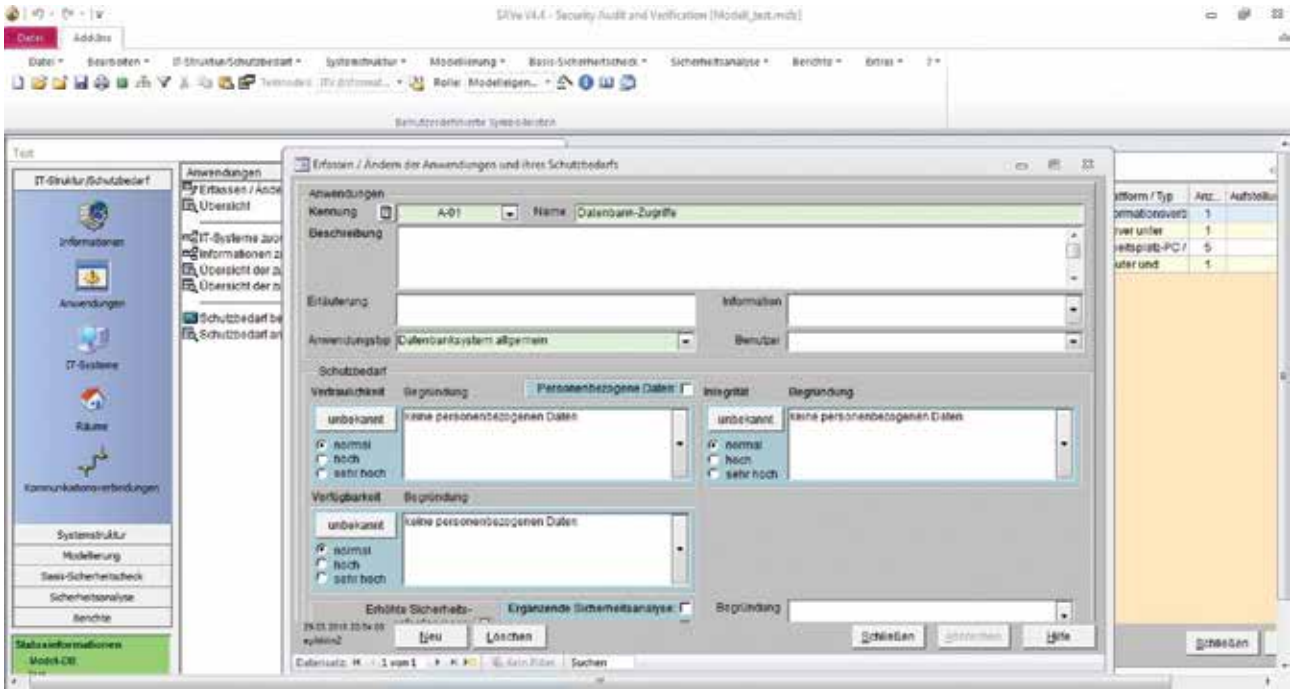


ABBILDUNG 16: ERFASSEN DER ZIELOBJEKTE IN DER IT-SICHERHEITSDATENBANK SAVe®

Der Import der Grundschutzkataloge ist nach einer gewissen Einarbeitungsphase und durch Nachlesen im technischen Handbuch einfach zu bewerkstelligen. Die Erstellung eines Informationsverbunds, das Erfassen der Stammdaten („Erhebung“) sowie die Verknüpfung mit Zielobjekten sind nach wenigen Klicks, Beschreibungen und Einstellungen realisiert. Nach erfolgreichem Verknüpfen der entsprechenden Zielobjekte und Einstellung des entsprechenden Schutzbedarfs kann man mit einem Klick (über den „Berechnen“-Button) den Schutzbedarf vererben und ggf. retrospektiv modifizieren (s. **ABBILDUNG 17**).

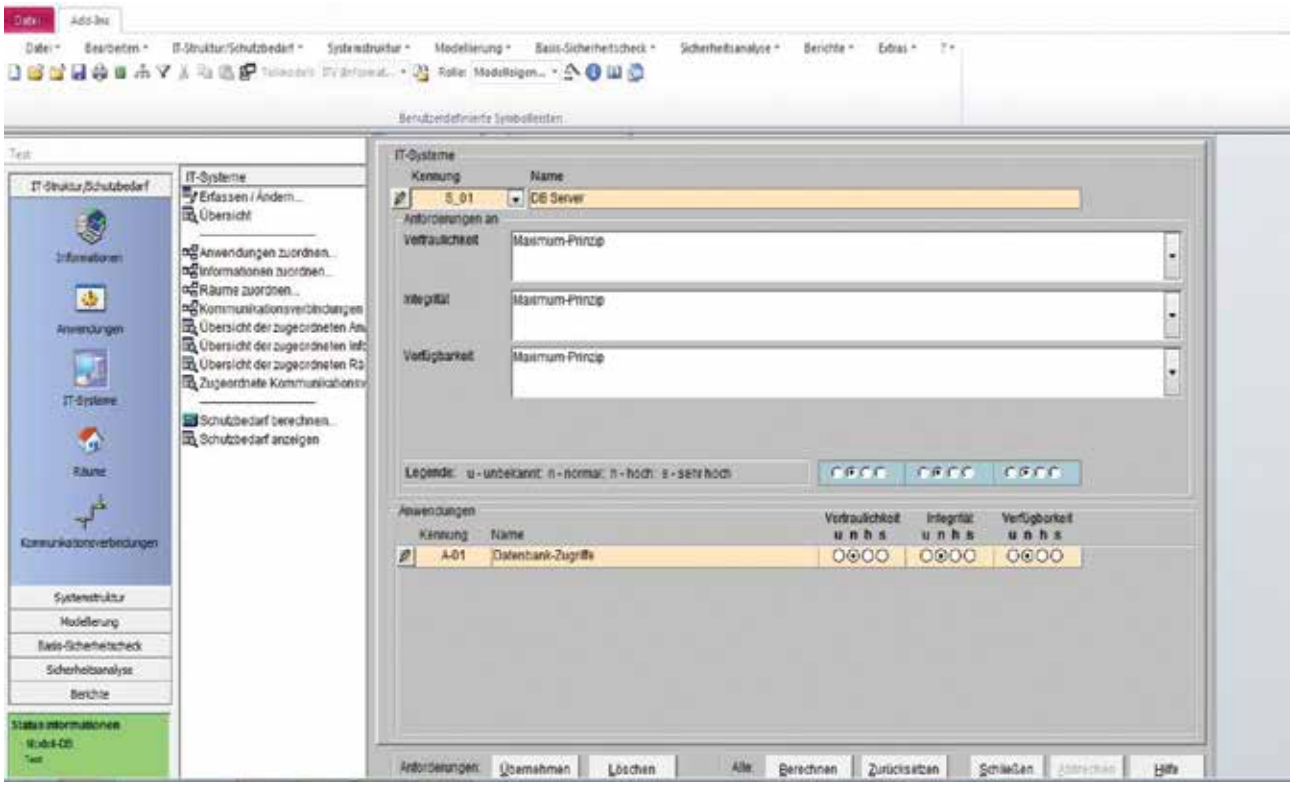


ABBILDUNG 17: VERERBUNG DES SCHUTZBEDARFS IN SAVe®

Das Importieren von Datenbeständen aus dem GSTOOL V4.8 war im Vergleich zu verinice nicht ohne weiteres möglich. Das könnte zum einen daran liegen, dass es sich um eine Testversion der IT-Sicherheitsdatenbank SAVe handelt. Zum anderen wird im Handbuch darauf hingewiesen, dass Datenbestände bis zur GSTOOL Version 4.7 unterstützt werden. Womöglich ist ein Import aus der aktuellen Version des GSTOOLs (V4.8) zumindest für Anfänger im Umgang mit der IT-Sicherheitsdatenbank ohne Support des Herstellers nicht ohne weiteres oder nur bedingt realisierbar. Des Weiteren sind die Schutzbedarfskategorien des BSI („normal“, „hoch“ und „sehr hoch“) zwar standardmäßig hinterlegt, jedoch nicht vordefiniert. Nach nochmaliger Rücksprache gab der Hersteller an, dass der Import von Datenbeständen aus dem GSTOOL problemlos und vollumfänglich funktioniert.

Das Modellieren des Informationsverbunds mithilfe der Bausteine aus den IT-Grundschutz-Katalogen des BSI ist einfach und übersichtlich. Die entsprechenden Bausteine werden einfach mit einem Häkchen versehen (s. **ABBILDUNG 18**). Nun muss nur noch der Umsetzungsstatus *(umgesetzt, teilweise umgesetzt, nicht umgesetzt oder entbehrlich)* für jede Maßnahme erfasst werden (s. **ABBILDUNG 19**).

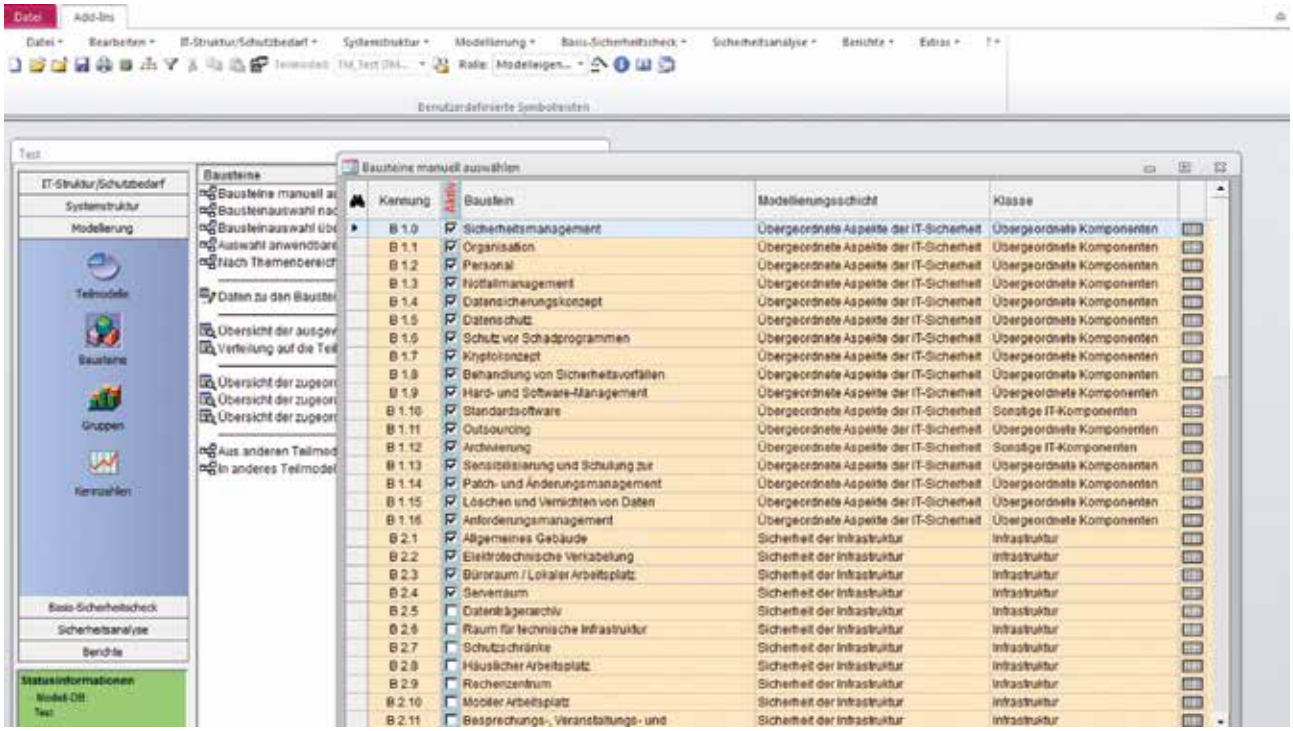


ABBILDUNG 18: MODELLIERUNG DES INFORMATIONSVERBUNDS IN SAVe®

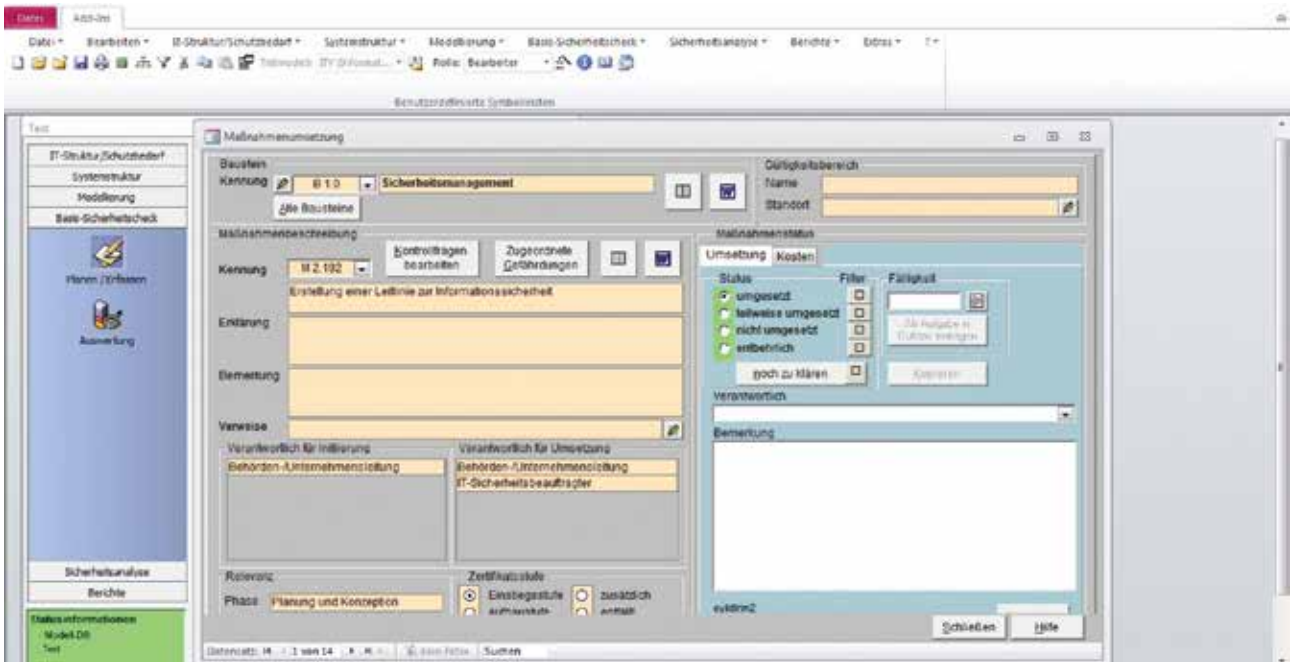


ABBILDUNG 19: UMSETZUNGSSTAND DER MAßNAHMEN IN SAVe® ERFASSEN

Nachdem der Umsetzungsstand der einzelnen Maßnahmen erfasst wurde, kann der Basis-Sicherheitscheck durchgeführt werden. **ABBILDUNG 20** zeigt beispielhaft wie der Basis-Sicherheitscheck in der IT-Sicherheitsdatenbank SAVe durchgeführt und angezeigt wird. Mithilfe weniger Klicks kann der Umsetzungsstand der Maßnahmen in der IT-Sicherheitsdatenbank schnell und einfach ausgewertet werden.

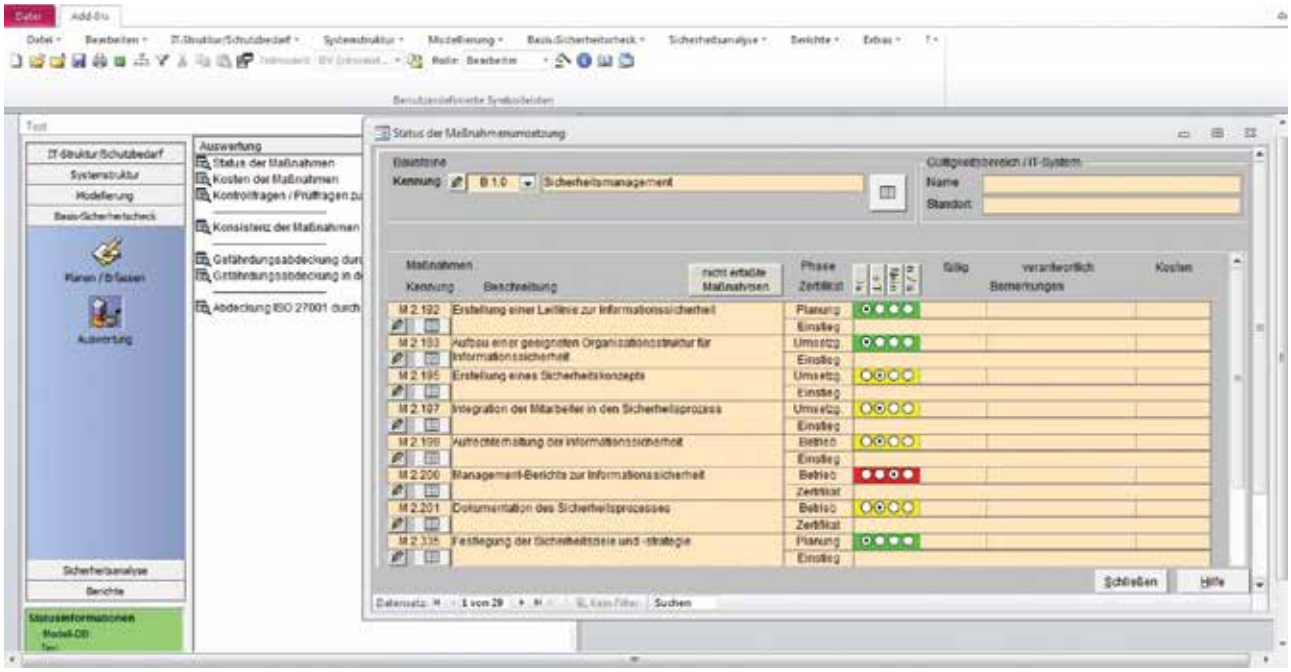


ABBILDUNG 20: BASIS-SICHERHEITSCHECK IN SAVe®

4.3 Zwischenfazit

Die Handhabung beider ISMS-Tools erwies sich nach einer gewissen Einarbeitung (4-8h) selbst für Anfänger als einfacher als erwartet. In beiden ISMS-Tools konnte der beispielhafte Informationsverbund (s. Kapitel 4.1 und 4.2) problemlos abgebildet und modelliert werden. Die methodisch korrekte Vorgehensweise nach IT-Grundschutz kann mit beiden ISMS-Tools gewährleistet werden. Strukturanalysen, Schutzbedarfsfeststellungen, Modellierung, Basis-Sicherheitscheck oder Realisierungsplanungen stellen keine große Herausforderung für beide Tools dar. Ergänzende Sicherheitsanalysen wurden im Zuge dieser Betrachtung nicht getestet.

Gerade bei verinice werden Nutzer des GSTOOLs viele Parallelen zum GSTOOL sehen. Wer jedoch eher mit der typischen Microsoft GUI vertraut ist, könnte die IT-Sicherheitsdatenbank SAVe bevorzugen. Selbstverständlich sprechen weitere Faktoren (z. B. die Auditfunktionalität) für den Einsatz von SAVe. Letztendlich ist es eine Frage der persönlichen Präferenz und der fachlichen Anforderung, welches ISMS-Tool das geeignetere ist.

5. EMPFEHLUNGEN/AUSBLICK

Wenn man rein hypothetisch davon ausgehen würde, dass es morgen zur endgültigen Einstellung des GSTOOLs respektive des Supports[2] kommt, gibt es viele geeignete Alternativen auf dem Markt.

Manche dieser Tools sind allerdings nicht in der Lage bestehende Datenbestände aus dem GSTOOL über geeignete Schnittstellen zu importieren, sodass – wie es bei manchen Organisationen erfahrungsgemäß oftmals der Fall ist – die über mehrere Jahre im GSTOOL gepflegten, überaus komplexen Informations-verbünde nicht weiter verwendbar sind. Falls es bei solchen Organisationen bzw. Informationsverbünden zu einem Wechsel des ISMS-Tools kommen sollte, müsste man entweder die Informationsverbünde – beginnend mit der erneuten Erfassung aller Stammdaten – komplett neu modellieren oder auf den meist kostenpflichtigen Support des jeweiligen Herstellers zurückgreifen. Es wird allerdings davon ausgegangen, dass diese Schwachstelle von den meisten Herstellern erkannt wurde und einige Hersteller sich auf solche Anforderungen – das Importieren von Datenbeständen aus dem GSTOOL – verstärkt konzentrieren. TABELLE 1 gibt einen Überblick darüber, welches der untersuchten Tools die Möglichkeit auf einen eigenständigen Import von Datenbeständen aus dem GSTOOL bietet. Außerdem wird eine Unterscheidung zwischen reinen ISMS-Tools und darüberhinausgehenden GRC-Tools vorgenommen.

Produkt	Typ	Eigenständiger Import von Datenbeständen aus dem GSTOOL
DHC Vision Information Security Manager 5.2	ISMS-Tool	Nein
GSTOOL 4.8	ISMS-Tool	Ja
HiScout GRC Suite 2.3	GRC-Suite	Ja (Support empfohlen)
iris (Version 15/R2 (Build 15107.1))	GRC-Suite	Nein
Opus-I (Oktober 2014)	ISMS-Tool	Ja
QSEC V4.2	GRC-Suite	Ja
SAVe V4.4 bzw. V5.0	ISMS-Tool	Ja
Sidoc (Oktober 2014)	ISMS-Tool	Nein
Verinice 1.9	ISMS-Tool	Ja

TABELLE 1: IMPORT VON DATENBESTÄNDEN AUS DEM GSTOOL

Neben der Frage nach einem geeigneten ISMS-Tool als Alternative zum GSTOOL stellt sich aus gegebenem Anlass auch die Frage, wie sich der ISMS-Tool-Markt entwickeln wird, wenn die Reformierung des IT-Grundschutzes, woran im BSI bereits seit längerem gearbeitet wird, vollzogen wurde. Nach bisherigem Kenntnisstand plant das BSI eine erhebliche Verschlankung der Bausteine auf 10 Seiten pro Baustein, die kurze Erstellungszeiten, einfache Aktualisierungen und verbesserte Lesbarkeit gewährleisten. Es ist anzunehmen, dass die Hersteller in der Lage sind die bei einer Reformierung bzw. Verschlankung des IT-Grundschutzes entstehenden Anforderungen zu erfüllen. Zunächst muss das BSI natürlich die neue, verschlankte Version des IT-Grundschutzes entwickeln und bekannt geben.

[3] Nach Angaben des BSI wird der Support des GSTOOLs voraussichtlich Ende 2016 endgültig eingestellt.

ANHANG - FRAGENKATALOG

Der folgende Fragenkatalog wurde von Experten aus dem IT-Grundschutzumfeld erstellt und an die Hersteller von ISMS-Tools zur Beantwortung verschickt.

SYSTEMVORAUSSETZUNGEN

Welche Betriebssysteme werden unterstützt (clientseitig)?

Angabe der von der Client-Software unterstützten Betriebssysteme

Antwort

O Windows 8
O Windows 7
O Windows Vista
O Windows XP
O Windows 2000
O Windows NT
O Mac OS
O Unix
O Linux

O sonstige:

Welche Betriebssysteme werden unterstützt (serverseitig)?

Angabe der von der Server-Software unterstützten Betriebssysteme

Antwort:

O kein Applikations-Server erforderlich
O lediglich ein Datei-Server erforderlich
O Windows Server 2012
O Windows Server 2008 R2
O Windows Server 2008
O Windows Server 2003
O Mac OS X Server
O Unix Server
O Linux Server

O sonstige:

Welche Datenbanken werden unterstützt?

Angabe der unterstützten Datenbanken

Antwort:

O Microsoft Access
O Microsoft SQL Server
O MySQL
O Postgres
O DB2
O Oracle

O sonstige:

Welche Hardware-Anforderungen bestehen für den Client?

Angabe der Anforderungen an die Hardware

Antwort:

Welche Hardware-Anforderungen bestehen für den Server?

Angabe der Anforderungen an die Hardware

Antwort:

BENUTZBARKEIT (USABILITY)

Ist das Tool/ Modul mandantenfähig?

Können mehrere IT-Infrastrukturen, z.B. von verschiedenen Kunden, durch das ISMS Tool konfliktfrei abgebildet werden? (Bezeichnungen, IT Verbund-Modell, Maßnahmenumsetzung etc. sind mandantenspezifisch zu verwalten)

Antwort:

Ist das Tool/ Modul mehrbenutzerfähig?

Ist die Benutzung des Tools durch mehrere Nutzer zu gleicher Zeit möglich? (5 oder mehr Nutzer).

Antwort:

Können Nutzer und deren Berechtigungen durch das Tool/Modul verwaltet werden?

Kurze Auskunft über die Nutzer und Berechtigungsverwaltung dieses Tools; auch bezogen auf eine ggf. vorhandene Mandantentrennung.

Antwort:

Ist das Tool/ Modul netzwerkfähig?

Basiert das Tool auf einem echten Client-Server Ansatz (Client-Anwendung kann auch ein Web-Frontend sein) (Server sollte ein Applikationsserver sein, nicht nur ein reiner Datenbank-Server) Kann das Tool auch über schmalbandige Verbindungen sinnvoll bedient werden?

Antwort:

Ist das Tool/ Modul offlinefähig?

Ist der Einsatz eines Client-Server basiertem ISMS-Tool auch ohne Netzwerkverbindung zum Server, zum Beispiel beim Kunden Vorort, möglich? Wie können die offline durchgeführten Änderungen später mit dem Server synchronisiert werden und welche Randbedingungen müssen dabei eingehalten werden?

Antwort:

Ist das Tool/ Modul mehrsprachig?

Welche unterschiedlichen Sprachen werden unterstützt? Sind diese Sprachen ggf. pro Benutzer separat konfigurierbar?

Antwort:

Können größere IT Verbünde problemlos modelliert und verwaltet werden?

Ist die Abbildung/Modellierung eines IT Verfahrens, welches beispielsweise mehrere Standorte (20 und mehr) oder viele Server (100 und mehr) umfasst, für das Tool/Modul machbar? Ist die Bedienbarkeit des Tools bzw. des Modells des IT Verfahrens danach noch gegeben (Antwortzeiten, weitere Ergänzungen, etc.)
Sie können auch gerne die oberen Limits der sinnvoll verwaltbaren Objekte angeben.

Antwort:

Gibt es Mobile Apps als Client Anwendungen?

Gibt es Apps, die eine mobile Nutzung der Anwendung per Smartphone/Tablet unterstützen? Wenn ja, bitte liefern Sie ein paar Details dazu.

Antwort:

UNTERSTÜTZUNG VON RISIKOANALYSEN

Bietet das Tool/Modul die Möglichkeit die Schutzbedarfsmatrix zu konfigurieren?

Sind die Kategorien sowie die Kriterien für die Einstufung des Schutzbedarfes frei definierbar? Wie viele Einstufungslevels für den Schutzbedarf können konfiguriert werden?

Antwort:

Ist die Schutzbedarfsfeststellung auf Geschäftsprozessebene mit Mapping auf IT-Objekte möglich?

Kann den IT Objekten der Schutzbedarf zugeordnet werden? Sind Vererbungsmechanismen für den Schutzbedarf von IT Objekten implementiert?

Antwort:

Wird manuelles Anpassen des automatisch ermittelten Schutzbedarfs durch das Tool/ Modul unterstützt??

Kann für ein IT Objekt der durch die Vererbungsfunktion automatisch ermittelte Schutzbedarf manuell überschrieben werden?

Antwort:

Wird eine klassische Bedrohungs- und Risikoanalyse durch das Tool/Modul unterstützt?

Besteht die Möglichkeit des Einpflegens einer Bedrohungsliste in das Tool, die über die Gefährdungskataloge des BSI hinaus gehen? Ist ein Zuordnen der Bedrohungen zu den IT-Objekten möglich? Kann die Eintrittswahrscheinlichkeit oder Eintrittshäufigkeit einer Bedrohung angegeben werden? Kann eine Risikomatrix konfiguriert werden? Können (automatisch) die Risiken für die IT-Objekte ermittelt werden?
Werden ggf. andere Arten von Risikoanalysen unterstützt (z.B. Schwergrad x Häufigkeit x Verwundbarkeit)

Antwort:

Werden ergänzende Maßnahmen durch das Tool/Modul unterstützt?

Besteht die Möglichkeit der Zuordnung von ergänzenden Sicherheitsmaßnahmen auf die IT Objekte, die über die IT Grundschutz-Kataloge hinaus gehen?

Antwort:

UNTERSTÜTZUNG IT-GRUNDSCHUTZ (BSI)

Sind die IT-Grundschutz-Kataloge des BSI standardmäßig hinterlegt?

Bitte ergänzen Sie auch noch, wie häufig ggf. eine Aktualisierung stattfindet.

Antwort:

Kann man die IT-Grundschutz-Kataloge / Ergänzungslieferungen eigenständig importieren oder ist man auf Updates/ Support des Herstellers angewiesen?

Antwort:

Ermöglicht das Tool/Modul das Erstellen eigener Bausteine, Gefährdungen und Maßnahmen?

Können neben den in den BSI IT-Grundschutz-Katalogen enthaltenen Bausteinen auch selbst definierte Bausteine, Gefährdungen und Maßnahmen in das ISMS Tool eingefügt werden? Bleiben diese Ergänzungen erhalten, wenn eine neue Ergänzungslieferung des BSI eingespielt wird?

Antwort:

Ermöglicht das Tool/Modul das Dokumentieren des Basis-Sicherheitschecks?

Unterstützt das ISMS Tool folgende Funktionalität:
Nach der Modellierung des IT Verbundes mit den vom BSI definierten Bausteinen erzeugt das ISMS Tool eine Liste der nach BSI IT-Grundschutz umzusetzenden Maßnahmen. Vom Auditor wird nun geprüft, ob und in welchem Umfang die Maßnahmen umgesetzt wurden. Der aktuelle Status wird dann der Auditor in das ISMS Tool eingetragen. Nach Abschluss des Audits sollte es möglich sein, mit dem ISMS Tool eine Maßnahmenliste mit dem aktuellen Implementierungsstatus zu erzeugen oder sich diese für den gesamten IT Verbund sowie für das einzelne IT-Objekt anzeigen zu lassen.

Antwort:

UNTERSTÜTZUNG ISO 27001

Unterstützt das Tool/ Modul den ISO 27001:2013 Standard (native)?

Besteht die Möglichkeit, mit dem Tool parallel oder alternativ statt BSI IT-Grundschutz, nach ISO 27001 zu arbeiten?

Es sollten alle Controls der ISO 27001:2013 Annex A im Tool implementiert sein.

Sind ggf. die Control Objectives und Implementation Guidelines aus ISO 27002 auch hinterlegt?

Antwort:

Unterstützt das Tool/ Modul den ISO 27001:2013 Standard (native)?

Besteht die Möglichkeit, zwischen einer BSI IT-Grundschutz-Sicht und einer ISO27001-Sicht hin- und her zu wechseln (für ein und denselben IT Verbund)?

Von einer konsistenten und redundanzfreien Datenerhebung bzw. –darstellung gehen wir dabei aus.

Antwort:

UNTERSTÜTZUNG VON ISMS MANAGEMENTPROZESSEN UND WORKFLOWS

Unterstützt das Tool/Modul Dokumenten-Management?
Können Dokumente (z.B. als Anhänge) durch das ISMS-Tool verwaltet und revisionssicher abgelegt werden? Besteht alternativ die Möglichkeit der Integration eines DMS-Systems (z.B. Sharepoint)
Antwort:

Wird eine automatische Versionierung bei Änderungen unterstützt?
Wird jede Änderung, auch an eingefügten Dokumenten, nachverfolgbar gespeichert? Wird ein Zugriff auf vorherige Versionen ermöglicht?
Antwort:

Bietet das Tool eine Workflow-Komponente oder kann es mit einem Workflow-System gekoppelt werden? Besteht alternativ die Möglichkeit, eMails mit einem Arbeitsauftrag an bestimmte Person(en) aus dem Tool heraus zu verschicken?
Antwort:

Besteht die Möglichkeit andere Tools zu integrieren?
Können Vulnerability Scanner integriert werden, um erkannte Schwachstellen unmittelbar im ISMS-Tool den entsprechenden IT-Objekten zuordnen zu können?
Antwort:

Werden Self-Assessments durch das Modul/ Tool unterstützt?
Können Self-Assessments (z.B. online mithilfe von generierten Webformularen) durchgeführt werden, um bestehende Maßnahmen hinsichtlich ihres Umsetzungsstatus beurteilen zu können? Besteht die Möglichkeit, den Benutzerkreis für dieses Self-Assessment völlig frei und unabhängig vom Benutzerkreis des Tools zu definieren? (z.B. basierend auf LDAP Benutzergruppen) Besteht die Möglichkeit, die Ergebnisse des Self-Assessments zu historisieren und so über die Jahre hinweg den Fortschritt erkennbar zu machen?
Antwort:

REPORTING

Verfügt das Tool/ Modul über eine Reporting-Funktion?
Können Reports, z.B. hinsichtlich des Schutzbedarfs, des IT Verbund-Modells, der Gefährdungen, der Maßnahmen und ihres aktuellen Umsetzungsstatus, etc., erzeugt werden?
Antwort:

Kann man Reports individuell konfigurieren?
Ist die Art (Aufbau der Tabellen und Grafiken) sowie der Informationsumfang der Reports frei konfigurierbar? Welche Einschränkungen bestehen hierbei?
Antwort:

Wird die Darstellung des Implementierungsstatus der Maßnahmen (BSI) bzw. der Controls (ISO 27001) durch das Tool/Modul unterstützt?
Ist insbesondere diese Darstellung als Report verfügbar bzw. kann erzeugt werden?
Antwort:

Verfügt das Tool über eine Microsoft Office® kompatible Import- und Exportfunktion?
Unterstützung gängiger Office-Formate für die Reports und ergänzend auch PDF
Antwort:

ÜBER CSC CYBERSECURITY

CSC ist ein führender globaler Anbieter von Informationssicherheit mit über 40 Jahren Erfahrung im privaten und öffentlichen Sektor.

Mit weltweit über 1.700 Informationssicherheitsexperten und 5+ Risk Management / Security Operations Center verfügt CSC über eines der breitesten Angebotsportfolios im Bereich Cybersecurity:

- Technische IT-Sicherheitsberatung (z.B. Penetrationstests, social engineering)
- Strategische & Operative Sicherheitsberatung (z.B. Risikomanagement)
- Identity & Access Management Beratung
- Managed Security Services (z.B. IAM, SOC, Netzwerke, Firewalls, DLP)
- Business Continuity Management & Disaster Recovery
- Application Security (z.B. Code reviews, SAP)
- Zertifizierungen (z.B. ISO, BSI, PCI, common critria labs)

KONTAKT

Vivian Haag

Cybersecurity Sales Lead Central Europe

vhaag@csc.com

Peter Rehäusser

Head of Cybersecurity Consulting Germany

prehaeus@csc.com

Lesen Sie über aktuelle Trends in der Cybersecurity http://www.21stcenturyit.de oder folgen Sie uns auf Twitter @CSC_Cyber oder @CSC_DE

Autoren der Studie:
Erkut Yildirim, Stephan Wolff, Yathursan Theva, Constanze Lissner, Peter Rehäußer

Regional CSC Headquarters

The Americas
3170 Fairview Park Drive
Falls Church, Virginia 22042
United States
+1.703.876.1000

Asia, Middle East, Africa
Level 9, UE BizHub East
6 Changi Business Park Avenue 1
Singapore 468017
Republic of Singapore
+65.6809.9000

Australia
26 Talavera Road
Macquarie Park, NSW 2113
Australia
+61(2)9034.3000

Central and Eastern Europe
Abraham-Lincoln-Park 1
65189 Wiesbaden
Germany
+49.611.1420

Nordic and Baltic Region
Retortvej 8
DK-2500 Valby
Denmark
+45.36.14.4000

South and West Europe
Immeuble Balzac
10 place des Vosges
92072 Paris la Défense Cedex
France
+33.1.55.707070

UK, Ireland and Netherlands
Floor 4
One Pancras Square
London
N1C 4AG
United Kingdom
+44.020.3696.3000

About CSC
CSC is a global leader in next-generation IT services and solutions. The company's mission is to enable superior returns on our clients' technology investments through best-in-class industry solutions, domain expertise and global scale. For more information, visit us at www.csc.com.