# ISIS12 – Informationssicherheit für mittelständische Unternehmen

Michael Gruber

BSP. SECURITY
michael.gruber@bsp-security.de

## Zusammenfassung

Verschiedene Informationssicherheits-Managementsysteme (ISMS) sind etabliert und werden in Organisationen als de-facto oder de-jure Normen eingesetzt. Parallel dazu existieren mit ITIL (IT Infrastructure Library) und dem ISO/IEC 20000 Standards und Normen, die den Bereich IT-Servicemanagement (ITSM) abdecken. Die bislang verbreiteten ISMS und ITSM stellen für mittelständische Unternehmen eine zu große Hürde für deren Einführung dar, zumal ein Managementsystem, das beide Sichten integriert, nicht vorhanden ist. Das neu entwickelte Managementsystem ISIS12 ist ein speziell für mittelständische Unternehmen konzipiertes praxisnahes Verfahrensmodell zur Etablierung und zum Betrieb eines ISMS mit integriertem ITSM. Das Vorgehensmodell wird durch ein speziell entwickeltes ISIS12-Softwaretool abgebildet. Optional ist eine Zertifizierung dieses Standards möglich.

# 1 ISMS light

ISIS12 (Informations SIcherheitsmanagement System in 12 Schritten) ist ein 12-stufiger Workflow zur Etablierung eines einfach einzuführenden Informationssicherheitsmanagementsystems. Dieses „ISMS light“ wurde speziell für mittelständische Unternehmen (ca. 100-1000 PC Arbeitsplätze) entwickelt. Es handelt sich um eine didaktisch verständliche Anleitung [ISIS12a], die bei der Umsetzung von ausgebildeten ISIS12- Consultants begleitet werden kann. Bei dem integrierten Managementansatz wird das ISMS mit einem ITSM verknüpft, eine Vorgehensweise, die bislang noch nicht in dieser Form vorgenommen wurde (vgl. [BSI05]). Das Verfahren kann auch als mögliche Vorstufe zur ISO/IEC 27001- bzw. BSI IT-Grundschutz-Zertifizierung zum Einsatz kommen.

Speziell für mittelständische Unternehmen wurde vom „**N**etzwerk für Informationssicherheit im Mittelstand“ (NIM) ISIS12 entwickelt. Die Entwicklung von ISIS2 durch NIM, bestehend aus 7 Unternehmen und 2 Hochschulen, wurde vom Bayerischen Staatsministerium für Wirtschaft, Infrastruktur, Verkehr und Technologie gefördert. Das Bayerische IT-Sicherheitscluster hat das Netzwerkmanagement übernommen.

Hierbei kam es zum Austausch von praxisnaher Projekterfahrung aus den Bereichen Informationssicherheit und IT-Servicemanagement mit wissenschaftlicher Theorie aus dem Bereich Wirtschaftsinformatik.

Das Vorgehensmodell ist fertig gestellt und wird bereits in den ersten Projekten eingesetzt. Im „Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand“ [ISIS12a] wird das ISIS12-Verfahren didaktisch aufbereitet beschrieben. Ein spezielles ISIS12 Softwa-

P. Schartner · P. Trommler (Hrsg.) · D•A•CH Security 2013 · syssec (2013) 275-281.

retool wurde an der Universität Regensburg vom Lehrstuhl I Wirtschaftsinformatik entwickelt, um die zu Grunde liegenden 12 Arbeitsschritte angeleitet durchführen zu können.

Ein speziell entwickelter ISIS12 Katalog [ISIS12b] wurde aus den BSI-Grundschutzkatalogen [BSI11a] und den Standards ISO/IEC 27001 und 27002 [ISO27002] abgeleitet. Abgestimmt auf die Erfordernisse mittelständischer Unternehmen werden darin in der Praxis bewährte Basis-Sicherheitsmaßnahmen zusammengefasst. Abgeschlossen werden kann die Etablierung des ISIS12-Managementsystems mit einer ISIS12-Zertifizierung. Die erste Etappe der „Tour de Security“ wäre geschafft.

# 2 Designkriterien

Bei der Entwicklung von ISIS12 wurde bewusst ein praxisnaher Ansatz gewählt. Das Verfahrensmodell wurde speziell für mittelständische Unternehmen entwickelt. Die Verhältnismäßigkeit der zu erbringenden Aufwände stand im Mittelpunkt der Überlegungen, ohne jedoch dabei die Informationssicherheit aus den Augen zu verlieren: „So einfach wie möglich, aber nicht einfacher!“

- Ziel war es dem Anwender einen konkreten Handlungsrahmen als Orientierung vorzugeben. So wurde der abstrakte Charakter der ISO/IEC 27001 durch ein konkretes Vorgehensmodell in 12 sequentiell zu durchlaufende Schritte ersetzt. ISIS12 bildet den Zyklus des zu etablierenden integrierten ISMS ab. Nach dem ersten „Durchlauf“ dient das Verfahrensmodell als Vorlage für interne und externe Audits und stellt somit die Aktualität und Optimierung des ISMS sicher.
- Bei ISIS12 werden dem Anwender konkrete Sicherheitsmaßnahmen an die Hand gegeben. Dazu wird der ISIS12-Katalog verwendet. Dieser wurde im Wesentlichen aus den BSI IT-Grundschutzkatalogen (vgl. [BSI11a]) und dem de-jure Standard ISO/IEC 270001 [ISO27001] (Maßnahmenziele A.5 – A.15) bzw. den Konkretisierungen in ISO/IEC 27002 [ISO27002] abgeleitet. Für die ISIS12-Zielgruppe (mittelständische Unternehmen) wurde die Fülle der vorgefundenen Sicherheitsmaßnahmen reduziert: Breitenwirkung, Umsetzbarkeit und trotzdem eine systematische Abdeckung von Gefährdungen standen für die Entwicklung des ISIS12 Katalogs im Mittelpunkt. Auch der Detailierungsgrad, zwischen BSI IT-Grundschutz (extrem) und der ISO/IEC 27001 (minimalistisch und abstrakt), wurde bewusst an die Zielgruppe der mittelständischen Unternehmen angepasst.
- Es wurde bewusst auf eine vorangestellte Risikoanalyse verzichtet, wie dies bei der ISO/IEC 27001 der Fall ist, da dieser basale Arbeitsschritt in der Praxis, nicht nur bei mittelständischen Unternehmen, zu größeren Problemen führen kann, die sich auf die daraus resultierende Sicherheitskonzeption negativ auswirkt. Auch nachgestellt wird wie bei der BSI IT-Grundschutzmethodik keine Risikoanalyse explizit angewandt (vgl. [BSI08c]). Vielmehr beinhaltet das an die BSI Grundschutzmethodik angelehnte Verfahren eine immanente Risikoanalyse: Die empfohlenen Sicherheitsmaßnahmen decken bereits einen Grundgefährdungskatalog ab.
- Durch den Einsatz eines speziell entwickelten ISIS12-Tools wird dem Anwender das Arbeiten mit dem Vorgehensmodell erleichtert werden. Das dafür entwickelte Tool bildet den ISIS12 Workflow komplett ab, liefert Hinweise für die einzelnen Arbeitsschritte und dokumentiert diese zugleich. Das ISIS12-Tool wird erfolgreich in ISIS12-Projekten eingesetzt und bietet neben einer Orientierung bei der Einführung des ISMS auch eine

wertvolle Basis für die nachfolgenden Revisionsaufgaben im Rahmen der PDCA-Systematik.

- Nicht nur das ITSM kann mit dem ISMS integriert werden, sondern auch weitere Managementsysteme können miteinbezogen werden. An erster Stelle ist das Datenschutzmanagement zu nennen. Hier kann die Konvergenz von Datensicherheit und Datenschutz institutionell etabliert werden. Zudem sind noch weitere integrierbare Managementsysteme denkbar. Einerlei ob es sich um bereits bestehende oder um noch zu etablierende Standards handelt. So etwa Qualitätsmanagement (ISO 9000) oder Umweltmanagement (ISO 14000), die bereits in zahlreichen mittelständischen Unternehmen Einzug gefunden haben.
- Das ISIS12 Managementsystem sollte zertifizierbar sein. Hierzu wurde ein eigenes Zertifizierungsschema entwickelt, das sich jedoch generell an der verbreitete Praxis der ISMS-Zertifizierung orientiert: Die Gültigkeit des Zertifikats beträgt drei Jahre und wird durch zwei Überwachungsaudits begleitet. Als exklusiven Zertifizierungspartner wurde mit der DQS GmbH ein entsprechender Vertrag geschlossen und DQS-Auditoren entsprechend ausgebildet.
- ISIS12 wurde zudem mit der Möglichkeit zur Skalierbarkeit entwickelt. Nach deren erfolgreicher Implementierung und optionalen ISIS12-Zertifizierung, steht der Weg in Richtung einer de-jure Zertifizierung nach „ISO/IEC 27001“ bzw. „ISO 27001 auf Basis von IT-Grundschutz“ offen.

# 3 Vorgehensmodell ISIS12

Aus langjähriger ISMS und ITSM Projekterfahrung der ISIS12 Architekten wurde das Vorgehensmodell in drei Grobphasen aufgeteilt. Vor den eigentlichen operativen Schritten, der Entwicklung der Sicherheitskonzeption (Phase 3), gilt es nach der Initialisierungsphase, zuerst die für den weiteren Verlauf notwendigen Voraussetzungen zu schaffen. Diese Vorgehensweise sichert einen reibungsloseren Projektverlauf bei der Implementierung des integrierten Managementsystems.

## 3.1 Initialisierung

ISIS12 ist als ein klassischer Top-Down-Ansatz konzipiert. Die Unternehmensleitung trägt dabei die Gesamtverantwortung für die Informationssicherheit, initiiert den dafür notwendigen Sicherheitsprozess und stellt die dafür erforderlichen Ressourcen zur Verfügung. Ohne diese Basis sind die weiteren Schritte nicht erfolgreich umzusetzen. Es besteht dann vielmehr die Gefahr, dass das Projekt scheitert.

**Schritt 1: Leitlinie erstellen**

Zu Beginn wird eine Leitlinie zur Informationssicherheit erstellt, die von der Unternehmensleitung als zentrales Strategiepapier unterzeichnet wird. Darin werden die den Geschäftszielen korrespondierenden Informationssicherheitsziele beschrieben, sowie die daraus abgeleitete Strategie fixiert. Den Mitarbeitern ist der Sinn dieser Leitlinie und die daraus resultierenden Konsequenzen zu vermitteln.

**Schritt 2: Mitarbeiter sensibilisieren**

Auf allen Organisationsebenen wird die Relevanz von ISIS12 für das Unternehmen auf zwei Ebenen kommuniziert:

a) Die Mitarbeiter werden über den ISIS12-Workflow informiert und auf die Bedeutung der Informationssicherheit für das Unternehmen hingewiesen. Sie werden regelmäßig über Neuerungen wie z. B. Bestellung des Informationssicherheits- bzw. Datenschutzbeauftragten, Änderungen der Leitlinie zur Informationssicherheit, Hinweise zu Sicherheitsvorfällen bzw. bzgl. Verhaltensfehler etc. informiert. Bei Nichteinhaltung der Leitlinie wird dies sanktioniert.

b) Der erweiterte Führungskreis wird zu Beginn der ISIS12-Implementierung über die auf die Mitarbeiter der verschiedenen Abteilungen zukommenden Arbeitsaufwände informiert. Bereits in dieser frühen Phase wird um die Mitarbeit der betroffenen Abteilungen „geworben".

## 3.2 Aufbau- und Ablauforganisation

Es ist sinnvoll und notwendig, dass in einer weiteren vorgelagerten Phase, also vor der eigentlichen Entwicklung und Umsetzung des Sicherheitskonzeptes, eine entsprechende Aufbau- und Ablauforganisation etabliert wird. Aus den Erfahrungen vieler durchgeführten Sicherheitsprojekten lässt sich die Erkenntnis ziehen, dass es ohne diese Vorarbeiten in der operativen Phase zu zeitlich erheblichen Verzögerungen kommt, da der eigentliche Projektverlauf unterbrochen werden muss, um zuerst Grundlagenaufgaben, wie etwa Dokumentationsaufgaben zu erledigen.

**Schritt 3: Informationssicherheitsteam aufbauen**

Die Zusammensetzung, die Aufgaben und Pflichten des Informationssicherheitsteams werden im Schritt 3 festgelegt. Die zentrale Rolle nimmt dabei der Informationssicherheitsbeauftragte (ISB) ein, der auch für die Einführung, Betrieb und Weiterentwicklung von ISIS12 verantwortlich ist. Bei der Zielgruppe der mittelständischen Unternehmen wird in der Regel der ISB seine Rolle im „Nebenamt" ausüben. Die Berichterstattung des ISB erfolgt, entsprechend der Stellung im Unternehmen, direkt an die Unternehmensleitung. Weitere Mitglieder können sein: Datenschutzbeauftragter, QM-Beauftragter, IT-Mitarbeiter, Anwender-Vertreter, externer ISIS2-Berater u.a.. Die Teammitglieder werden in dieser Phase mit der ISIS12-Methodik vertraut gemacht.

**Schritt 4: IT-Dokumentationsstruktur**

Es wird, falls noch nicht im Unternehmen vorhanden, eine Struktur für die IT-Dokumentation im Unternehmen entwickelt und eingeführt. Neben formalen Festlegungen wie etwa Versionierung und verpflichtende Dokumenteninformationen werden verbindliche Rahmendokumente als Basis für das IT-Betriebshandbuch und IT-Notfallhandbuch erarbeitet. Bei bereits etablierten QM-Systemen wird das dort entwickelte und vorhandene System zur „Lenkung von Dokumenten und Aufzeichnungen" für ISIS12 adaptiert.

**Schritt 5: IT-Service Management Prozesse**

Für das Vorgehensmodell ISIS12 sind drei generische IT-Service-Managementprozesse verbindlich einzuführen: Wartung, Änderung und Störungsbeseitigung. Diese drei Basisprozesse greifen auf eine einzuführende „Configuration Management Data Base" (CMDB) zu. Die CMDB enthält u. a. die Anforderungen an die IT-Systeme und Infrastruktur aus ISIS12 Schritt 7 (MTA und SLA) in Form eines Service-Katalogs. Es werden hierbei generische Prozessbeschreibungen für eventuell neu einzuführende Serviceprozesse zur Verfügung gestellt.

## 3.3 Operative Arbeiten

Nach den Vorarbeiten in den vorangegangenen Phasen beginnt mit Schritt 6 der „operative“ Teil des ISIS12 Vorgehensmodells, der Konzeption und Implementierung der integrierten Sicherheitskonzeption.

**Schritt 6: Kritische Applikationen identifizieren**

Es werden zunächst unternehmenskritische Anwendungen lokalisiert und identifiziert. Deren Schutzbedarf wird jeweils bezogen auf die Grundwerte „Vertraulichkeit, Integrität und Verfügbarkeit“ bewertet. Ein Verfahren, das stark an den BSI IT-Grundschutz angelehnt ist. Allerdings wurde die zum Einsatz kommenden Schutzbedarfskategorieszenarien von sechs auf vier reduziert und die originäre Ratingskala „normal“, „hoch“ und sehr „hoch“ wurde durch die neutralen Stufen „A“, „B“ und „C“ ersetzt, um mögliche Umfrageartefakte zu vermeiden.

Daraus werden die Maximal Tolerierbare Ausfallzeit (MTA) und die Service Level Agreements (SLA) abgeleitet, die im Service-Katalog dokumentiert werden. Zudem wird die Verarbeitung personenbezogener Daten erfasst. Die Ergebnisse werden im ISIS12-Tool erhoben und festgehalten. Diese Informationen werden in den folgenden Schritten weiter verarbeitet.

**Schritt 7: IT-Struktur analysieren**

Nach der Lokalisierung unternehmenskritischer Anwendungen werden die für den operativen Betrieb erforderlichen technischen, personellen, organisatorischen und infrastrukturellen Objekte ermittelt. Diese werden in sicherheitsrelevanter Abhängigkeit zu den kritischen Applikationen erfasst und mit den Anwendungen aus Schritt 6 verknüpft. Damit kann der zuvor ermittelte Schutzbedarf der kritischen Applikationen, inkl. MTA und SLA, diesen Objekten vererbt werden: „ISMS meets ITSM“. Neben dem Prinzip der Vererbung des maximalen Wertes werden auch Verteilungs- und Kummulationseffekte betrachtet.

**Schritt 8: Sicherheitsmaßnahmen modellieren**

Nun erfolgt die Zuordnung der empfohlenen Sicherheitsmaßnahmen aus dem ISIS12-Katalog zu den im vorangegangen Schritt ermittelten Objekten. Dies geschieht mit dem ISIS12-Tool automatisch. Der speziell angepasste ISIS12 Katalog wurde aus dem BSI-Grundschutzkatalog und dem Standard ISO/IEC 27001 (Maßnahmenziele A.5– A.15) bzw. den Konkretisierungen in ISO/IEC 27002 abgeleitet. Speziell für den Mittelstand wurde die Fülle, der in den genannten Standards vorgefundenen Sicherheitsmaßnahmen reduziert: Breitenwirkung, Umsetzbarkeit und trotzdem eine systematische Abdeckung von Gefährdungen durch korrespondierende Sicherheitsmaßnahmen, standen für die Entwicklung des ISIS12-Katalogs im Mittelpunkt. Der Detailierungsgrad zwischen BSI IT-Grundschutz (extrem hoch) und der ISO/IEC 27001 (minimalistisch und abstrakt) wurde bewusst auf die Zielgruppe der mittelständischen Unternehmen angepasst.

Bei Bedarf besteht in dieser Phase des Vorgehendmodells die Möglichkeit benutzerdefinierte Bausteine in den Katalog zu integrieren, soweit dies erforderlich erscheint. So wäre etwa der Baustein Videokonferenz zwingend notwendig, wenn regelmäßig Forschungsergebnisse via Videokonferenzsitzungen zwischen Firmenstandorten ausgetauscht werden würden. Ziel ist es, die für das mittelständische Unternehmen erforderlichen Sicherheitsmaßnahmen zu ermitteln. Es entsteht dadurch zunächst ein spezifisch angepasster Prüfplan.

**Schritt 9: Ist-Soll Vergleich**

Im Ist-Soll-Vergleich wird der Umsetzungsgrad, der in Schritt 8 empfohlenen Maßnahmen untersucht. Der aktuelle Umsetzungsgrad wird mit „ja“, „teilweise“, „nein“ oder „nicht notwendig“ bewertet. Ziel ist es die noch nicht vollständig umgesetzten erforderlichen Sicherheitsmaßnahmen zu identifizieren, da diese in den weiteren Schritten noch wirksam umzusetzen sind. Bereits vollständig umgesetzte Maßnahmen („ja“) und entbehrliche Maßnahmen werden an dieser Stelle bereits mit einem Revisionsdatum versehen, um diese dann im Rahmen des PDCA-Zyklus zu einem späteren Zeitpunkt erneut auf Wirksamkeit und Angemessenheit überprüfen zu können.

**Schritt 10: Umsetzung planen**

Die noch ganz oder teilweise umzusetzenden Sicherheitsmaßnahmen werden zunächst konsolidiert, dann priorisiert und zusammen mit einer Kostenplanung der Geschäftsleitung als Entscheidungsvorschlag präsentiert. Nach Festlegung des Umsetzungszeitraums und der Umsetzungsreihenfolge werden diese im ISIS12 Schritt 11 final umgesetzt.

**Schritt 11: Umsetzung**

Die genehmigten Sicherheitsmaßnahmen werden wirksam umgesetzt. Für jede Maßnahme wird die Rolle des Initiators, des Umsetzers und der Zeitpunkt der finalen Realisierung festgelegt. Eine begleitende Schulung der Mitarbeiter unterstützt die Einführung der Sicherheitsmaßnahmen.

**Schritt 12: Revision**

Im „abschließenden“ Schritt werden im Sinne des PDCA-Prinzips (Plan-Do-Check-Act) die Aktualität der ISIS2-Schritte 1-11 und die wirksame Umsetzung der noch offenen Sicherheits-Maßnahmen im Sinne einer Revision kontinuierlich untersucht. Das ISMS light ist etabliert und wird durch interne Audits kontinuierlich weiter optimiert.

# 4 Zertifizierung

Wie bereits beschrieben war die Möglichkeit einer optionalen ISIS12-Zertifizierung ein Design-Kriterium zu Beginn der Entwicklung. Die Zertifizierung verfolgt extern den Zweck Geschäftspartnern die Qualität des etablierten Managementsystems intersubjektiv belegen zu können. Intern trägt eine Zertifizierung dazu bei das ISMS ständig wirksam und aktuell zu halten und es kontinuierlich zu optimieren. Als Exklusivpartner zur Zertifizierung konnte die DQS GmbH gewonnen werden. Das Auditierungs- und Zertifizierungsschema wurde in Zusammenarbeit mit der DQS GmbH erstellt. Das Zertifikat hat eine Gültigkeit von drei Jahren. In diesen drei Jahren finden zwei eintägige Überwachungsaudits statt. Im dritten Jahr kann durch ein Rezertifizierungsaudit das Zertifikat erneuert werden. Die Zertifizierung wird in der Regel nach einem zweitägigen Audit durch zertifizierte und speziell geschulte ISIS12-Auditoren durch die DQS erteilt.

# 5 Zusammenfassung

Mit ISIS12 steht mittelständischen Unternehmen ein speziell für ihre Bedürfnisse entwickeltes ISMS mit integriertem ITSM zur Verfügung. Das zu etablierende Sicherheitskonzept basiert auf bewährten Standards für Informationssicherheit, wurde jedoch entsprechend „mittelstandstauglich“ adaptiert. Ein speziell entwickeltes ISIS12-Tool unterstützt den Anwender bei der ISIS12 Etablierung, dokumentiert die erbrachten Arbeiten und kann als Werkzeug für die Durchführung interner und externer Audits verwendet werden.

Durch eine optionale ISIS12-Zertifizierung kann das Engagement im Bereich Informationssicherheit Geschäftspartnern gegenüber demonstriert werden. Ein Wettbewerbsfaktor, der speziell für mittelständische Unternehmen immer wichtiger wird. Das etablierte ISMS light kann skaliert werden. Und die nächste Etappe der „Tour de Security“ wartet schon mit den Hochgebirgsetappen ISO/IEC 27001 oder dem BSI IT-Grundschutz.

Durch ISIS12 ist es mittelständischen Unternehmen möglich, sich den Herausforderungen der Zukunft im Bereich Informationssicherheit im Rahmen ihrer Möglichkeiten zu stellen. Und nicht nur für KMU. Es wird aktuell geprüft, inwieweit ISIS12 auch im Behördenbereich zum Einsatz kommen kann – als mögliche Vorstufe zum BSI IT-Grundschutz.

## Literatur


[BSI05] Bundesamt für Sicherheit in der Informationstechnik, ITIL und Informationssicherheit. Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management, 2005.

[BSI08a] Bundesamt für Sicherheit in der Informationstechnik, Managementsysteme für Informationssicherheit (ISMS), BSI-Standard 100-1, Version 1.5, 2008.

[BSI08b] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, 2008.

[BSI08c] Bundesamt für Sicherheit in der Informationstechnik, Risikoanalyse auf Basis von IT-Grundschutz, BSI-Standard 100-3, Version 2.5, 2008.

[BSI11a] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kataloge, 12. Ergänzungslieferung, 2011.

[BSI11b] Bundesamt für Sicherheit in der Informationstechnik, Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz, 2011.

[ISIS12a] ISIS12, Handbuch zur effizienten Gestaltung von Informationssicherheit im Mittelstand, ISIS12, V1.3, 2013.

[ISIS12b] ISI12 Katalog. Sicherheitsmaßnahmen zur Informationssicherheit im Mittelstand, V1.2, 2012.

[ISO27001] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements, 2008.

[ISO27002] ISO/IEC 27002, Information technology – Security techniques – Code of practice for information security management, 2008.