IT-Notfallmanagement „ISMS-Notfall“ Aus der Praxis für die Praxis

Herman Huber

J. Schmalz GmbH
herman.huber@schmalz.de

Zusammenfassung

Die J. Schmalz GmbH ist der weltweit führende Anbieter in der Automatisierungs-, Handhabungs- und Aufspanntechnik und bietet Kunden aus zahlreichen Branchen innovative und effiziente Lösungen aus dem Bereich der Vakuum-Technik. Das Unternehmen beschäftigt am Hauptsitz in Glatten (Schwarzwald) und in 16 Niederlassungen im Ausland mehr als 900 Mitarbeitende. Mit der Einführung eines Sicherheitsmanagementsystems (ISMS) will sich das mittelständische Unternehmen international vor Zugriffen schützen. Das Projekt sollte auch der Thematik Datenschutz nach deutschem Datenschutzniveau gerecht werden. Im Detail werden die Einführung und Umsetzung des Teilprojekts „IT-Notfallmanagementsystem auf Grundlage eines bereits vorhandenen Ticketing Systems“ erläutert. Als mittelständisches Unternehmen mussten neben engen Budgetgrenzen auch knappe Personalressourcen berücksichtigt werden. Trotzdem sollten hohe Qualitätsansprüche im internationalen Umfeld erfüllt sein. Eine mittelfristig angestrebte Zertifizierung im Bereich der IT-Sicherheit musste ebenso berücksichtigt werden. Der IT-Notfallprozess soll in das Tagesgeschäft der IT-Abteilung integriert werden und nicht als gesondertes Thema in unregelmäßigen Abständen als Projekt auftauchen.

1 Theorie

In den vergangenen Jahren wurden im Bereich des IT-Notfallmanagements und des IT-Sicherheitsmanagements sowohl in der Forschung, als auch in der Industrie sehr stark konträre Meinungen diskutiert und untersucht. Während die Forschung primär daran interessiert war, theoretische Modelle zu entwickeln, orientierte sich die Industrie sehr stark an den konkreten Bedürfnissen von Unternehmen. Diese versprachen sich von einem standardisierten und pragmatischen Prozessablauf (angesichts immer komplexerer Infrastrukturen) zeitliche Einsparungen und effizienteres Arbeiten in Verwaltungstätigkeiten. Eine Einhaltung gesetzlicher Vorgaben musste dabei erfüllt werden. Die Zielsetzung der Untersuchungen war somit sehr unterschiedlich. Das führte dazu, dass zwischen den beiden Herangehensweisen eine große Lücke entstand und auch heute oft noch besteht.

Das Projekt wurde in einem klassisch mittelständischen Unternehmen realisiert – eine Verbesserung der Ist-Situation sollte dabei möglichst schnell erreicht werden.

Die Projektleitung hat in der Initiierungsphase sieben Tage für die Recherche sowohl im Internet, als auch im deutschen Forschungsnetz und in verschiedenen wissenschaftlichen Bibliotheken benötigt. Dabei ist ein auf theoretischen Erkenntnissen basierender Projektplan entstanden. In einer zweiten Phase von 14 Tagen wurden verschiedenste Aspekte berücksichtigt und Dienstleister aus dem Bereich Business Continuity und Notfallvorsorge eingeladen und zur Vorstellung ihrer Vorgehensweise aufgefordert. Die Erkenntnisse flossen in den Projektplan ein. In

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 222-230.

einer dritten Phase von sieben Tagen wurden diese Erkenntnisse und die Gegebenheiten innerhalb des Unternehmens (Ist-Situation, Ticketsystem Vorort) im Projektplan berücksichtigt.

Danach wurden das Projektbudget, die Ressourcen und die Ziele festgelegt. Wichtig war in dieser Phase bereits die Erkenntnis, dass es sich nicht um ein technisches Projekt sondern um ein zu ca. 80 % organisatorisches Projekt handelt.

1.1 Fragestellungen zu Beginn des Projekts

- Wie kann ein mittelständisches Unternehmen aus dem laufenden Tagesbetrieb seine Prozesse so umstellen, dass keine zu große Belastung für die Mitarbeitenden entsteht?
- Wie können wir im Projekt die Mitarbeitenden von der Einführung eines restriktiven IT-Notfallmanagementsystems überzeugen?
- Besitzt die Aufbau- und Ablauforganisation den entsprechenden Reifegrad für eine solche Veränderung?
- Wie schaffen wir es, Verantwortlichkeiten (Owner) für einzelne, wichtige und sensible Bereiche zu definieren?
- Wie können wir die sensiblen Bereiche der Firma identifizieren? (Stichwort: Wenn die Firma wüsste, was die Firma weiß.)
- Wie erzielen wir Nachhaltigkeit durch Anpassungen der Unternehmensprozesse im Sinne der Problemstellung?
- Wie kommen wir schnell zu messbaren Ergebnissen?
- Wie hoch sollten wir das Projektbudget ansetzen?
- Wie bekommen wir alle Applikationen bezüglich des IT-Notfallmanagements harmonisiert?
- Können wir uns dieses Projekt überhaupt leisten und ist es jetzt der richtige Zeitpunkt zur Einführung?

1.2 Realisierungsschritte

- Bewusstsein für die „Sensibilisierung“ in der gesamten Firma mit Schwerpunkt in der IT-Abteilung schaffen.
- Spezielle Schulungen im Tagesgeschäft für das IT-Personal integrieren.
- Initiierung des Notfallmanagementprozesses mit Benennung eines IT-Notfallmanagers.
- Umsetzung des Notfallmanagementprozesses in einzelnen Phasen.
- Übergabe in die Linienfunktion.
- Einführung eines Managementsystems zu den Themen IT-Notfallmanagement, Datenschutz, IT-Sicherheit → IT-Compliance.

1.3 Was ist neu?

Sämtliche Vorgaben wurden nach dem BSI-Grundschutzkatalog (100-4, M 6 Notfallvorsorge) im vorhandenen Ticketsystem in einer eigenen Projektumgebung eingebaut und mit einer Wiedervorlagefunktion (sechs Monate) versehen.

- Der IT-Notfallmanagementprozess ist in das Tagesgeschäft der IT-Abteilung integriert. Zum Großteil ist es nicht mehr als explizite Notfallvorsorge erkennbar.

- Vollautomatische Wiedervorlagefunktion (alle sechs Monate, Zeit kann variabel gewählt werden) für IT-Notfallvorgänge mit eingebautem Qualitätsprüfungsprozess.
- Standardisierte Dokumentenvorlage mit Historienfunktion.
- Automatischer Abgleich der Dokumente aus dem vorhandenen MS-SharePoint-Umfeld in das Ticketsystem.
- Vollautomatische Erzeugung eines Clone des Ticketsystems mit allen Dokumenten auf ein spezielles Notfallnotebook in einer separaten Brandschutzzone.
- Automatisch generiertes Notfallhandbuch aus den Dokumenteneinträgen der einzelnen Tickets auf Knopfdruck und bei Bedarf.
- Zusätzliche Sicherung der Dokumentenumgebung auf zwei verschlüsselten USB Sticks:
  - Stick 1: Ablage Tresor
  - Stick 2: Zugriff durch IT-Notfallmanager
- Nutzung der Relationsmöglichkeit des Ticketsystems, um Schnittstellenfunktionen zu dokumentieren. (Stichwort „Abhängigkeiten von Hardware und Software im Netzwerk mit Visualisierung“).
- Nutzung der CMDB des Ticketsystems für die IT-Notfalldokumentation.
- Visualisierung der Systemlandschaft.
- Integration des Notfallmanagementprozesses in den Service-Desk-Prozess. (Störung → Notfall → Krise → Katastrophe).

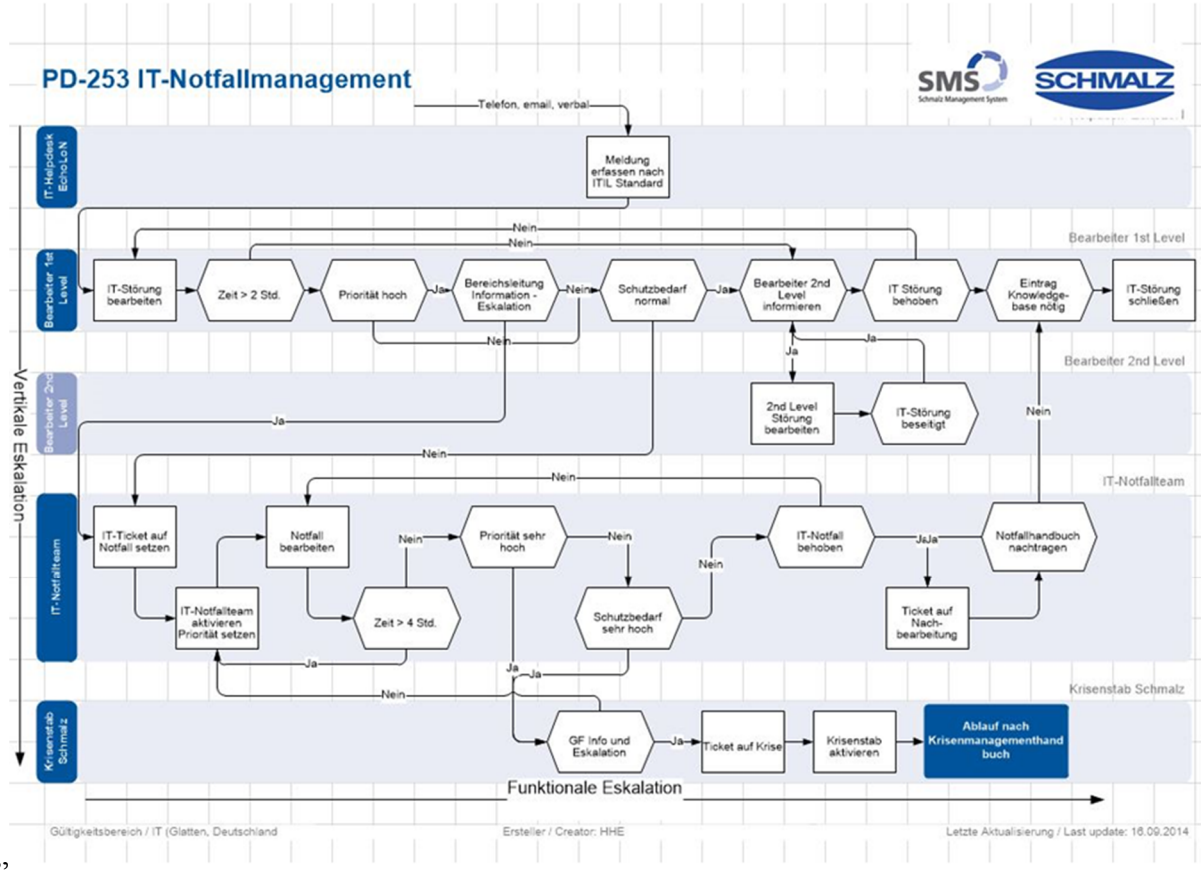

Abb. 1: PD-253 IT-Notfallmanagement (Prozessdokumentation)

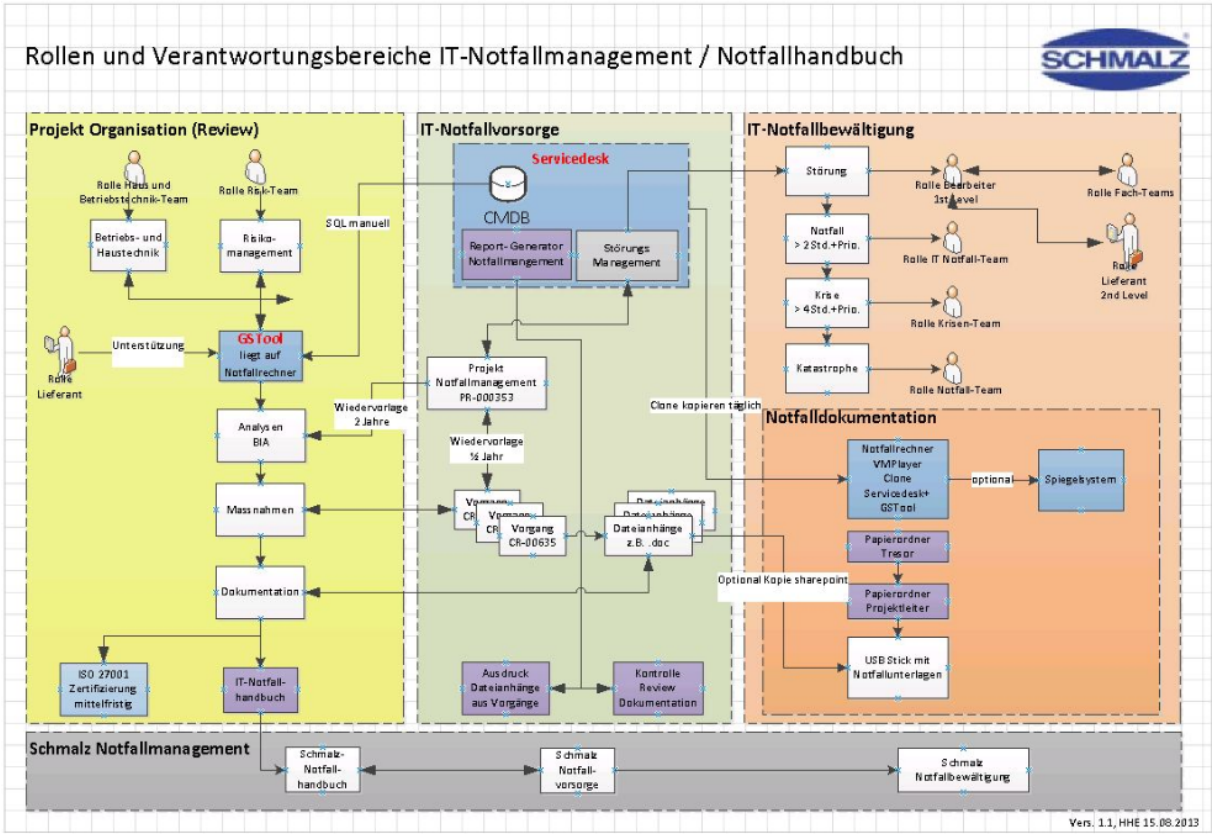

Abb. 2: Rollen und Verantwortlichkeiten

2 Beschreibung des Sicherheitskonzepts

2.1 Inhalte

Um die einzelnen Themen besser fassen und strukturieren zu können, wurde folgende Kategorisierung der Bereiche vorgenommen, bereits umgesetzt bzw. befindet sich in der Einführung. Im Einzelnen werden nur Stichworte der Einzelbereiche genannt.

2.2 Personelle Maßnahmen

- Ernennung eines Datenschutzbeauftragten (01.07.2013):
  - Phase I nur Deutschland
  - Phase II ab 01.01.2014 international
- Ernennung eines IT-Notfallbeauftragten (01.10.2013):
  - IT Deutschland
- Ernennung eines IT-Sicherheitsbeauftragten (13.10.2014):
  - International
- Ernennung eines Schmalz Notfallbeauftragten / Koordinator (01.12.2014):
  - Phase I nur Deutschland

2.3 Technische Maßnahmen

- Einführung neuer Firewallsysteme.

- Verschlüsselung aller Notebooks.
- Einführung einer WLAN-Lösung am Standort Glatten (Zertifikat basierend).
- Einführung E-Mail-Verschlüsselung für kritische Bereiche (zentrale Firmenlösung).

2.4 Organisatorische Maßnahmen

- Schulungen:
  - Datenschutz (durchgeführt durch den Datenschutzbeauftragten):
    - Regelprozess für alle neuen Mitarbeitenden, 1 x im Monat
    - Alle Mitarbeitenden (beginnend, Führungskräfte, Administratoren, Personal, Vertrieb, Marketing etc.) ca. 40 x seit Juli 2013
    - Weiterbildung des Datenschutzbeauftragten zum Auditor, 3 x seit Juli 2013
  - IT-Sicherheit (durchgeführt durch IT-Sicherheitsbeauftragten):
    - Regelprozess für alle neuen Mitarbeitenden, 1 x Monat
    - IT Personal Deutschland 5 x seit Juli 2013
    - IT Personal international 2 x seit Oktober 2014
    - Alle Geschäftsführer international 2 x seit Juli 2013
    - Weiterbildung BSI-Veranstaltung für den IT-Sicherheitsbeauftragten, 2x seit Juli 2013
  - Schulungen innerhalb der Schmalz Academy (Schnittstelle Privat-Beruf, durchgeführt von IT-Sicherheitsbeauftragtem) pro Halbjahr:
    - Bequem shoppen und sicher bezahlen
    - Cloud Computing
    - Datenschutz für Nachzügler
    - Datenverschlüsselung E-Mail & Co.
    - Industrie 4.0 und Security
    - Kinderschutz bei neuen Kommunikationstechniken
    - Philosophie der Zeit „Mensch – Maschine – Schnittstelle“
    - Sicheres Surfen im Netz
    - Soziale Netzwerke
    - Suchmaschinen – Wer (richtig) sucht, der findet
  - Zentrale Informationsveranstaltung durch den Verfassungsschutz:
    - Obere und mittlere Führungsebene 2 x seit November 2014
  - IT-Notfallmanagement:
    - 5 x Kleinschulungen in Teamsitzungen der IT-Abteilung
    - Verhalten bei Notfällen und IT-Sicherheitsvorfällen 4 x seit Juli 2013
  - 2 x pro Jahr werden bei Veranstaltungen des Unternehmens IT-Informationen an die Geschäftsführer der Auslandsgesellschaften weitergegeben.
- Beitritt Mitglied Allianz für Cyber-Sicherheit (Informationen und Veranstaltungen).
- Fachbereiche einbinden.
- Einführung einer zentralen Telefonnummer zu Fragen des Datenschutzes und der Datensicherheit.
- Zentrale E-Mail für Anfragen und Warndienste.
- E-Mailverteiler (Sicherheitslage und Aktivitäten der Firmengruppe):
  - Monatlicher Lagebericht an Führungskräfte und Administratoren

  - Quartalsbericht an Auslandsgesellschaften
  - CERT Meldungen „sehr hoch“ und „hoch“ werden in das Ticketsystem der Firma übernommen.
- Ansprechpartner festlegen (Woher bekommen wir Informationen?):
  - Kontakt zu Landesdatenschutzbeauftragten herstellen
  - Kontakt zu BSI herstellen
  - Kontakt zu Landesverfassungsschutz herstellen
  - Kontakt zu Anwalt herstellen (festlegen)
  - Kontakt zu Polizeibehörden /LKA herstellen (notieren)
- Auslandsgesellschaften:
  - Assessment
    - Self Assessment nach Fragekatalog
    - Vor Ort Audit durch Administratoren oder IT-Leitung
- Dienstleister Selektion:
  - Festlegung von IT-Dienstleister IT-Security

2.5 Strategie

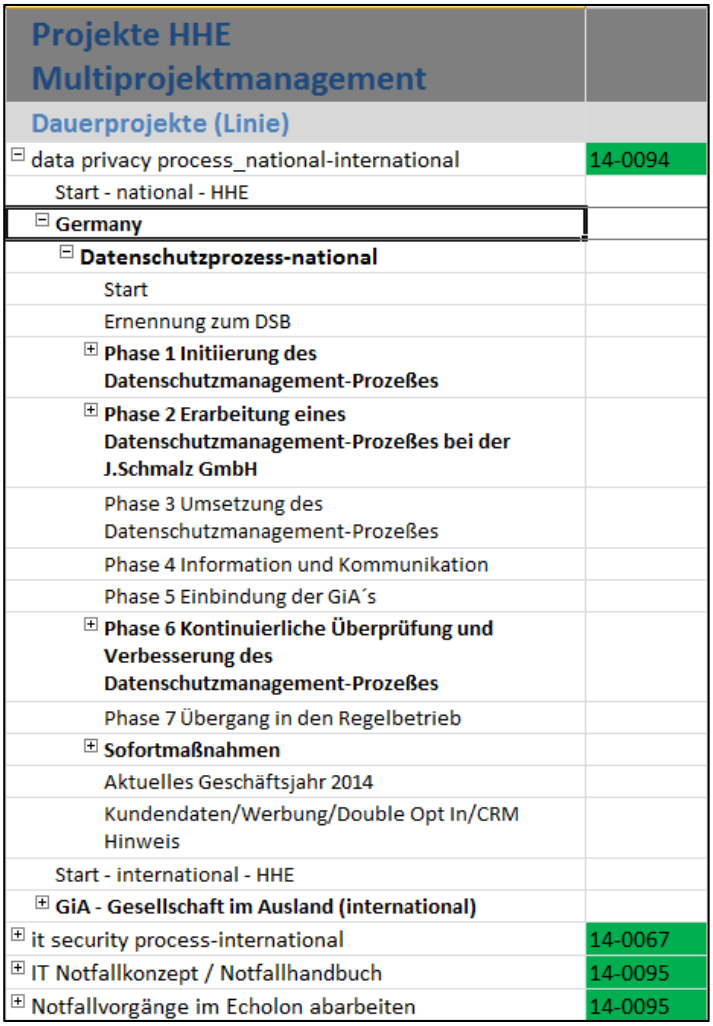

Abb. 3: Auszug aus Projektplan

Zu Beginn der Tätigkeit zum 01.07.2013 wurde mit der Geschäftsführung ein initialer Projektplan zur Einführung eines Datenschutzprozesses national und in der zweiten Phase ab 01.01.2014 international festgelegt. Aus diesem resultieren die im Einzelnen genannten Aktivitäten und Projekte – unter anderem die Einführung eines IT-Notfallmanagements.

2.6 Regelungsbereiche

Sowohl der Datenschutzbeauftragte als auch der IT-Sicherheitsbeauftragte sind direkt der Geschäftsleitung als Stabsstelle unterstellt. Das IT-Notfallmanagement und der IT-Notfallbeauftragte unterstehen der IT-Leitung.

2.7 Verknüpfung von Qualitätssicherung und Sicherheit

Innerhalb des Ticketsystems wurde im Prozessablauf eine separate Qualitätsprüfungsstufe eingeführt. Nach Abschluss der Dokumentation des Sachbearbeiters bekommt der IT-Notfallbeauftragte eine Aufforderung zur Prüfung des Vorgangs. Erst nach erfolgter Prüfung wird der Vorgang als erledigt gekennzeichnet. Nach sechs Monaten erfolgt eine Wiedervorlage beim Sachbearbeiter.

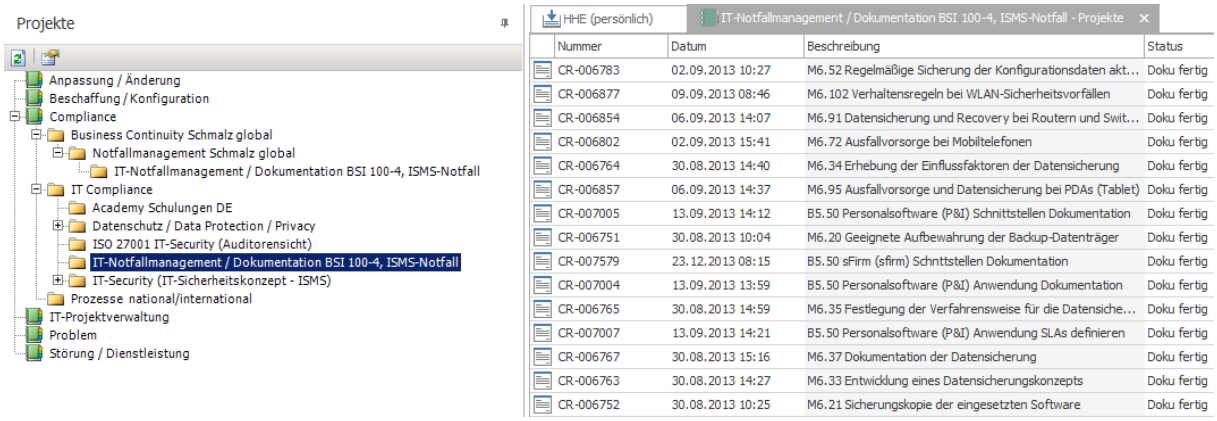

Abb. 4: Auszug aus dem Ticketsystem

Weil der IT-Notfallbeauftragte gleichzeitig der IT-Sicherheitsbeauftragte ist, fließen nötige Sicherheitsaspekte unmittelbar in die Dokumentation mit ein. IT-Sicherheitsvorgänge, IT-Notfallvorgänge und Datenschutzvorgänge sind hierbei eng miteinander verwoben.

3 Aufwand und Risiken

3.1 Realisierung

Nach Start des Projekts war es nötig, den beteiligten Personenkreis (IT-Abteilung, Führungskräfte, Mitarbeitende) in immer wiederkehrenden Aktivitäten für die Thematik zu sensibilisieren. Die Geschäftsführung sprach das Thema deshalb konsequent an und die IT-Leitung sowie der Datenschutzbeauftragte sensibilisierten die Mitarbeitenden kontinuierlich. Ohne ein klares Willensbekenntnis zu dieser Thematik, in dieser kurzen Zeit – vor allem von Seiten der Geschäftsführung – ist ein solches Thema nur schwer einzuführen und in die laufenden Prozesse zu integrieren.

3.2 Aufwände

Das Initialprojekt ging 2013 über fünf Monate und nahm ca. 320 Stunden in Anspruch.

Der IT-Notfallbeauftragte betreute das Projekt 2014 mit 124 Stunden (ohne Tests und Übungen), das ist ein monatlicher Arbeitsaufwand von ca. 10 Stunden.

4 Erfolg bzw. Mehrwert des Konzeptes

4.1 Stellungnahme Dritter

Während des Überwachungsaudits ISO 9001:2008, durchgeführt durch die DEKRA vom 22. bis 24.09.2014, wurde das neue IT-Notfallmanagementsystem angelehnt an den BSI Standard unter dem Punkt 3 „Besondere Aspekte des Auditberichts“ positiv hervorgehoben.

4.2 Übertragbarkeit auf andere Bereiche

Durch die starke Vereinheitlichung und Anpassung auf die Belange eines klassischen deutschen Mittelständlers sind die hier dargestellten Prozesse und die Vorgehensweise sehr schnell auf andere Unternehmungen übertragbar. Es wurde Wert darauf gelegt, die Auslandsgesellschaften bereits frühzeitig in die Prozesse zu integrieren.

5 Ergebnis

Die Einführung eines IT-Sicherheitsmanagementsystems (ISMS) ist eine unternehmensweite, organisatorische Veränderung, die von den Mitarbeitenden nicht immer als Chance gesehen wird. Vor allem dann, wenn es den eigenen Bereich betrifft und man als Konsequenz Einbußen im Rahmen der derzeitigen Tätigkeiten befürchtet. Die Mitarbeitenden verstehen die Veränderung aus betrieblicher Sicht oft nicht und ziehen sich auf Argumente oder Fragen wie „Funktioniert doch, wieso etwas ändern?“ oder „Werde ich jetzt nicht mehr gebraucht?“ zurück und „blockieren“ dadurch den Fortschritt. Fehlende oder mangelhafte organisatorische und personelle Maßnahmen führen zu diesen Widerständen, die durchaus ein ernstzunehmendes Projektrisiko darstellen.

Diesem Umstand kann durch gezielte Kampagnen und Veranstaltungen entgegengewirkt werden. Die Darstellung der Vorteile für das Unternehmen, aber auch für jeden Einzelnen, sowie laufende Informationen aus dem Projektbüro helfen hier, das Momentum der Erneuerung aufrecht zu erhalten.

Durch die erreichte Selbstverpflichtung der Mitarbeitenden gegenüber den Zielen des Unternehmens und dem Projekt ist es erst möglich, die oft sogar komplexen Aufgabenstellungen für den Projekterfolg zu bewältigen.

Aus heutiger Sicht kann man die Einführungsphase des IT-Sicherheitsmanagementsystems (ISMS) – und hier explizit das Teilprojekt IT-Notfallmanagement – als vollumfänglich geglückt bezeichnen. Kritische Stimmen sind heute kaum noch wahrnehmbar. Die einzelnen Aufgaben und Tätigkeiten sind in das Tagesgeschäft übergegangen.

6 Fazit

Im deutschen Mittelstand läuft vieles anders. Hoher zeitlicher Druck und knappe Projektressourcen stellen besonders hohe Anforderungen an das Projekt. Der Faktor Mensch und eine sensible, vorsichtige Vorgehensweise ist ein ausschlaggebender Faktor für die Akzeptanz und den Erfolg des Projekts.

Das Projekt als soziales System ist methodisch in der Lage, Projektrisiken auf der Basis von Umweltanalysen festzustellen und zu minimieren. Es gibt genau zwei Aspekte warum Projekte scheitern können: Technik und (menschliche) Kommunikation. Zu Beginn des gegenständlichen Projekts wird die Technik nur rudimentär betrachtet. Daher ist die Kommunikation neben anderen menschlichen Aspekten als Erfolgsfaktor zu betrachten. Denn Tools machen keine Projekte – Menschen machen Projekte und sichern den messbaren Erfolg.

Literatur

[BuSi14] Bundesamt für Sicherheit in der Informationstechnologie, IT-Grundschutz-Kataloge 2014 EL 14 DE (2014),

[GSW+09] Grünendahl, Steinbacher, Will: Das IT-Gesetz: Compliance in der IT-Sicherheit, Springer Vieweg, Wiesbaden, (2009, 2012)

[GDD+10] Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) Datenschutz im Unternehmen, GDD, Bonn, (2010)

[MoK+09] K. Molitorisz: BRBAC-Rollenbasierte Zugriffskontrolle für Unternehmen, VDM Verlag Dr. Müller, Saarbrücken (2009)

[GiK+13] K. Gießner: Sicherheit durch rollenbasierte Rechteverwaltung(2013) www.betasystems.com (13.03.2013)

[WiR+13] R. Wiltscheck: Digitale Identitäten, Rollen und Rechte (2013) http://www.channelpartner.de/a/digitale-identitaeten-rollen-und-rechte, 2618798 (08.11.2013)

[ReT+09] T. Reeb: Governance, Risk, Compliance (2009) http://www.compliancemagazin.de/produkte/identitymanagement/econet080609.html (08.06.2009)

[GrA+07] A. Gropp: Seminararbeit Rollenbasierte Zugriffskontrolle, Institut für Programmierstrukturen und Datenorganisation (IPD), Universität Karlsruhe (2007)