Toolgestützte Assessments zu Datenschutz und Datensicherheit in kleinen und mittelständischen Unternehmen

Matthias Rodeck, Caroline Voigt, Arndt Schnütgen
BEL NET GmbH
matthias.rodeck@belnet.de, caroline.voigt@belnet.de,
arndt.schnuetgen@belnet.de

Ina Schiering, René Decker
Ostfalia Hochschule für angewandte Wissenschaften
i.schiering@ostfalia.de, rene.decker@ostfalia.de

Abstract: In kleinen und mittelständischen Unternehmen sind Datenschutz und Datensicherheit eine besondere Herausforderung. Zum einen sind diese Unternehmen geprägt durch dynamische Änderungen von Prozessen und IT-Services, zum anderen ist es notwendig einen Überblick zu erhalten und auf sich ändernde Rechtslagen zu reagieren. Das Management von Datenschutz und Datensicherheit basiert in diesen Unternehmen derzeit meist auf der Fachkunde des Datenschutzbeauftragten unterstützt durch Assessments, die sich auf Fragebögen oder auf Fragebögen basierende Tools stützen. Dieses Vorgehen ist aufwändig und wenig flexibel. Hier wird ein Ansatz vorgestellt, Datenschutzbeauftragte durch eine Kombination aus einem IT-Service zusammen mit einem mobilen Client zu unterstützen, die auf BPMN basierende abstrahierte Darstellungen von Prozessen in den Mittelpunkt von Assessments stellt.

Keywords: Datenschutz, Datensicherheit, BDSG, Assessment, Pattern, BPMN, IT-Service, mobiler Client

1 Einleitung

Um sich der Frage des Datenschutzes in Bezug auf kleine und mittelständische Unternehmen (KMU) zu nähern, ist es zunächst wichtig, die Struktur und Arbeitsweise solcher Unternehmen zu betrachten. Im Vergleich zu großen Unternehmen, ist ein wesentlicher Unterschied die größere Flexibilität. Bezogen auf die Produkte und Dienstleistungen, stellt diese Flexibilität genau den Marktvorteil dieser Unternehmen dar. Sie sind dadurch in der Lage, zeitnah auf Kundenbedürfnisse einzugehen oder kleine Veränderungen an Produkten vorzunehmen, wenn der Markt dahingehenden Bedarf signalisiert.

Die Flexibilität entsteht unter anderem dadurch, dass Entscheidungswege kurz sind. Führungskräfte des Unternehmens sind ansprechbar, Hierarchieebenen sind flach gehalten. Informationen werden aus diesem Grund leichter auch ohne Berechtigung zwischen den Abteilungen und Hierarchieebenen ausgetauscht.

Aus Sicht des Datenschutzes können genau diese Flexibilität und die kurzen Wege problematisch sein: So kann es zu Zugriffen auf personenbezogene Daten, wie z. B. Daten von Mitarbeitern oder Kunden kommen, weil ein Mitglied der Unternehmensleitung diese Daten einsehen möchte oder man sich unter Kollegen unbürokratisch hilft. Da es wenig schriftlich niedergelegte Richtlinien und Prozesse gibt, werden Entscheidungen wie der Einsatz von Videoüberwachung aufgrund von Diebstählen oder die Nutzung von komfortablen Cloud-Diensten wie Dropbox, Google Docs, GMail oder Siri getroffen, ohne die Auswirkung und den rechtlichen Rahmen in Bezug auf personenbezogene Daten zu berücksichtigen.

Ziel dieser Arbeit ist es, eine Tool-Unterstützung für Assessments im Bereich Datenschutz und Datensicherheit vorzustellen, die besonders die hier dargestellte Situation in KMU im Fokus hat. Bisher werden meist Fragebögen verwendet oder Tools, die im wesentlichen auf Fragebögen basieren. Ein solches Vorgehen ist wichtig, um eine möglichst vollständige Darstellung zu bieten. Besonders erfahrene Datenschutzbeauftragte weichen in der Praxis von diesen relativ starren Verfahren ab und entwickeln persönliche Vorgehensweisen.

Hier wird der Ansatz der Patterns vorgestellt. Sie bilden typische Ausprägungen von Verfahren für die Verarbeitung personenbezogener Daten und werden dargestellt als BPMN (Business Process Management Notation) Diagramme. Diese Patterns werden zusätzlich um Hinweise auf mögliche Schwachstellen innerhalb der einzelnen Verfahren ergänzt. Dabei wird versucht einen Kompromiss zu finden, zwischen Übersichtlichkeit, Transparenz für das Gespräch mit Ansprechpartnern und ausreichender Tiefe, so dass das Tool als roter Faden für Gespräche genutzt werden kann. Wichtiges Ziel dieses Vorgehens ist es, den Datenschutzbeauftragten mit Fachkunde in seiner Arbeit zu unterstützen. Zu dem Ergebnis des Assessments können anschließend innerhalb des Backends des IT-Services Maßnahmen zugeordnet werden. Unterstützt wird dies durch Hinweise zu Maßnahmen, die bereits in ähnlichen Situationen verwendet wurden. Damit ist dieser Ansatz geeignet qualitätsgesichertes Arbeiten zwischen mehreren Datenschutzbeauftragten zu ermöglichen und unterstützt besonders Personen mit z.B. technischem und juristischen Hintergrund bei der Zusammenarbeit. Der mobile Client und das Backend wurden als IT-Service innerhalb des Projekts „Datenschutz-Cloud“ entwickelt und werden derzeit bei einem Unternehmen aus dem Projektkonsortium getestet.

In Kapitel 2 werden kurz rechtliche Rahmenbedingungen für den Datenschutz in Deutschland und vorhandene Tools, sowie Vorgehensweisen für Datenschutz und Datensicherheit dargestellt. Im folgenden Kapitel 3 wird der Ansatz erläutert, typische Ausprägungen von Verfahren durch Patterns darzustellen. Anschließend wird in Kapitel 4 das Vorgehen bei einem Assessment mithilfe der Datenschutz-Cloud vorgestellt. Dann wird erläutert, wie die Sammlung von Patterns erstellt und weiterentwickelt werden kann (Kapitel 5). Außerdem wird die Architektur der Datenschutz Cloud dargestellt (Kapitel 6). Abschließend wird der hier vorgestellte Ansatz bewertet und ein Ausblick gegeben.

2 Hintergrund

Auch für kleine und mittelständische Unternehmen ist die Verarbeitung großer Datenmengen heutzutage Teil des Unternehmensalltags. Neben der Schaffung innerbetrieblicher Organisationsstrukturen zur effizienten und bedarfsgerechten Verarbeitung und Speicherung von Informationen, sehen sich die Unternehmen auch einer Reihe von rechtlichen Vorgaben gegenübergestellt. Im vorliegenden Kontext betrifft dies die Verarbeitung personenbezogener Daten.

Unter personenbezogenen Daten versteht man Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, vgl. § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) [BDS]. Darunter fallen Informationen wie Name, Adresse, Kontonummer, Telefonnummer oder auch die IP-Adresse[1]. Einfachgesetzlich geregelt finden sich eine Vielzahl von Vorschriften zum Schutz personenbezogener Daten im BDSG, daneben z.B. auch im Telemediengesetz (TMG) und im Telekommunikationsgesetz (TKG). Für die Evaluation des hier vorgestellten Prototypen eines IT-Services, der Assessments im Bereich des Datenschutzes und der Datensicherheit unterstützt, konzentrieren wir uns auf das BDSG.

Zusammenfassend seien als Grundprinzipien des Datenschutzes basierend auf dem BDSG nach Bizer [Biz07] zu nennen:

- Rechtmäßigkeit der Verarbeitung personenbezogener Daten
- Einwilligung der betroffenen Personen
- Zweckbindung bei der Verarbeitung personenbezogener Daten
- Erforderlichkeit bezogen auf die für den Zweck notwendigen Daten und die Dauer der Speicherung
- Transparenz der Datenverarbeitung aus Sicht der Betroffenen
- Datensicherheit (s.u.)
- Kontrolle der Einhaltung der gesetzlichen Rahmenbedingungen durch Datenschutzbeauftragte und Aufsichtsbehörden

Besonders bzgl. der Datensicherheit werden in Anlage 1 zu § 9 BDSG Anforderungen für die Bereiche Zutrittsschutz, Zugangsschutz, Zugriffsschutz, Schutz bei der Übermittlung, Protokollierung, Kontrolle des Auftragsdatenverarbeiters, Verfügbarkeit der Daten und das Trennungsgebot formuliert.

Gemäß § 4d, § 4e des BDSG muss die Verarbeitung personenbezogener Daten dokumentiert werden. Dieses geschieht üblicherweise in einem Verfahrensverzeichnis, dass mindestens die Angaben nach § 4e enthält.

[1] Strittig, zum Streitstand siehe [LT12]

Bei der Realisierung des Datenschutzes in diesem dynamischen Umfeld werden als Basis derzeit häufig Fragebögen eingesetzt, wie z. B. der Baustein Datenschutz im IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) [Bun13]. Wobei dabei ein vollständiges Informationssicherheits-Managementsystem (ISMS) im Vordergrund steht, das die Anforderungen gemäß ISO/IEC 27001 [ISO13] umfasst. Zu diesem sehr umfangreichen Vorgehensmodell gibt es die Variante ISIS12 [Gru13], die besonders kleine und mittelständische Unternehmen im Fokus hat. Sowohl für IT-Grundschutz, als auch für ISIS12, kann als Tool-Unterstützung zur Modellierung des Informationsverbunds und zum Ausfüllen der Fragebögen das Tool *verinice*[2] verwendet werden.

Des Weiteren werden fokussiert auf den Bereich des Datenschutzes Tools wie z. B. *2B Secure*[3] oder *privacyGUARD*[4] eingesetzt, die ebenfalls im Wesentlichen auf dem Ausfüllen von Fragebögen basieren.

Ein weiteres Beispiel für den Einsatz von Werkzeugen für die Beurteilung von Datenschutz und Datensicherheit ist das Tool CARiSMA [HWP+13]. Hier liegt der Fokus auf der Prüfung von Geschäftsprozessen in Cloud Services basierend auf dem Risikomodell der IT-Grundschutz Kataloge unter Verwendung von Ontologien. Alle diese Vorgehensweisen haben eine möglichst vollständige Abbildung des Bereichs im Fokus. Einen etwas anderen Ansatz verfolgen Privacy Impact Assessments (PIA), siehe z.B. [Off09], [fISB11] oder [WDH12]: Bei PIAs wird nicht abschließend ein fertiggestellter IT-Service überprüft oder ein Status erhoben, wie bei den bisher vorgestellten Ansätzen, sondern ein Projekt ab der Entstehung eingebettet in das Risikomanagement begleitet.

3 Patterns zu Datenschutz und Datensicherheit

Alle in Kapitel 2 vorgestellten Ansätze zu Assessments im Bereich Datenschutz und Datensicherheit für kleine und mittlere Unternehmen haben die Vollständigkeit der Darstellung im Fokus. Damit stellen sie gute Leitlinien für Personen mit wenig Erfahrung dar und ermöglichen zudem Vergleiche mit anderen Organisationen bzw. innerhalb der Organisation zu verschiedenen Zeitpunkten.

Der hier vorgestellten Ansatz hat zum Ziel, eine Darstellung zu finden, die dauerhaft als roter Faden in den Gesprächen des Assessments genutzt werden kann und dabei Übersicht und Transparenz fördert. Dazu wurde die Idee der Patterns genutzt. Dabei geht es darum, wiederverwendbare Lösungen für wiederkehrende Probleme zu finden. Dieses Konzept wurde zuerst von Alexander [AIS77] im Bereich der Architektur vorgeschlagen. In der Informatik wurden in vielen Bereichen Patterns entwickelt, z.B. Software Design Patterns von Gamma et al. [GHJV94], Security Patterns [YWM08] und Privacy Patterns [DG12].

Bezogen auf Assessments im Bereich Datenschutz, stellen die Verfahren wiederkehrende Punkte dar. Besonders bei kleinen und mittelständischen Unternehmen kommen zum größten Teil wiederkehrende Verfahren im Umgang mit Mitarbeiter- bzw. Kundendaten

[2] http://www.verinice.org/
[3] http://www.2b-advice.com/
[4] http://www.privacyguard.de/

vor, wie z.B. die Zeiterfassung, das Führen einer Personalakte oder der Umgang mit Bewerbungen. Zu den Workflows, die diesen Verfahren zugrunde liegen, werden auf BPMN (Business Process Management Notation) [Bus11] basierende, abstrahierte Darstellungen erarbeitet, welche die für die Beurteilung des Datenschutzes wichtigen Aspekte darstellen. Diese Modellierungen werden als *Patterns* bezeichnet. Zu jedem Verfahren kann es mehrere Ausprägungen geben, die durch Patterns beschrieben werden, wie z.B. Zeiterfassung realisiert durch elektronische Geräte oder papierbasierte Verfahren. Zusätzlich zu der Darstellung des Workflows werden Hinweise auf potentielle Schwachstellen ergänzt. Diese werden als Ellipsen dargestellt, die durch gestrichelte Linien mit Aktivitäten des Workflows verknüpft werden. Dabei wird nicht der volle Umfang der BPMN verwendet. Lediglich Start- und Endereignis, Aktivitäten, Gateways und ein Sequenzfluss zwischen den Elementen sind möglich.

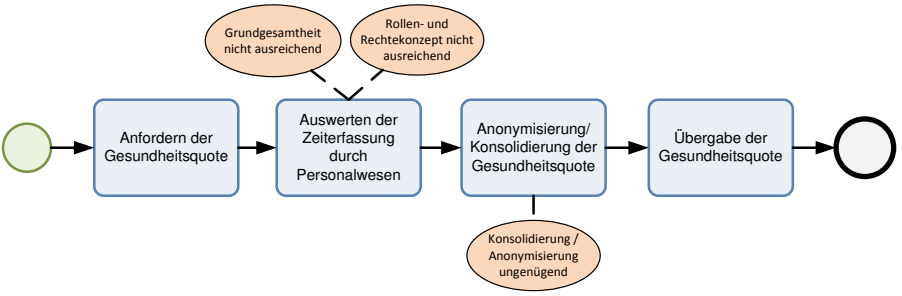

Abbildung 1: Controlling der Gesundheitsquote

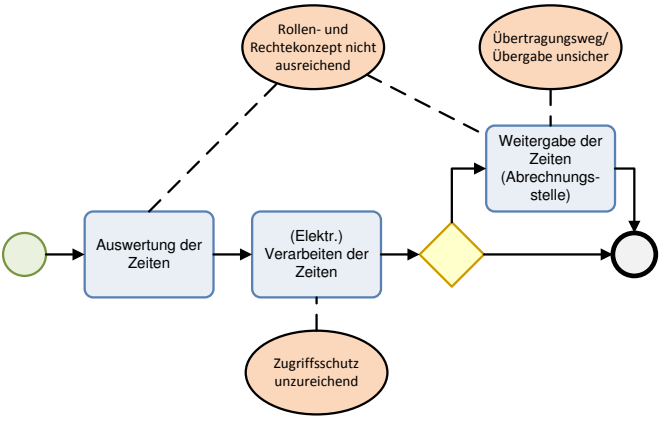

Abbildung 2: Zeiterfassung - elektronische Erfassung der Arbeitszeiten von Arbeitnehmern

Es ist wichtig zu beachten, dass es sowohl zu einer Aktivität mehrere potentielle Schwachstellen geben kann, als auch eine Schwachstelle, wie z.B. das unzureichende Rollen- und Rechtekonzept in Abbildung 2 bei mehreren Aktivitäten vorkommen kann.

Dadurch können Verfahren in Form von Patterns abgebildet werden. Weiterhin ist es notwendig im Bereich der technisch-organisatorischen Maßnahmen eine Reihe von typischen potentiellen Schwachstellen zu prüfen, die nicht direkt mit einzelnen Verfahren in Verbindung stehen. Zum Beispiel werden in Abbildung 3 potentielle Schwachstellen im Zusammenhang mit dem Zutritt zum Gelände, Gebäude oder kritischen Bereichen einer Organisation dargestellt.

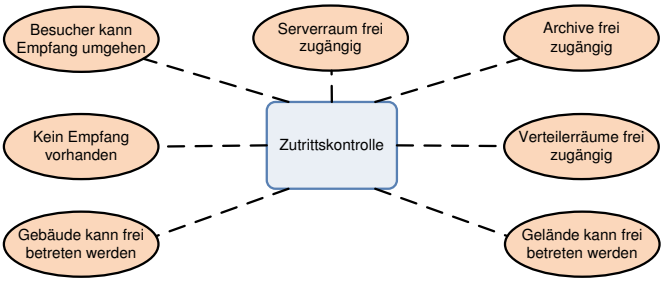

Abbildung 3: Potentielle Schwachstellen im Bereich Zutritt

Andere Bereiche mit ähnlichen Anforderungen sind z.B. Sicherung von Räumen, Verfügbarkeit, Zugriffsschutz. Hierbei wurde eine an BPMN-Diagramme angelehnte Darstellung gewählt, bei der das Thema in Form einer Aktivität in der Mitte steht und von potentiellen Schwachstellen umgeben wird. Gibt es mehr Schwachstellen, als in dieser Art darstellbar, werden die Schwachstellen thematisch gruppiert und auf mehrere Patterns verteilt.

Die Sammlung aller Patterns wird als *Patternpool* bezeichnet. Im Patternpool werden zusätzlich Schwachstellen und Maßnahmen bezogen auf Schwachstellen unabhängig von Patterns gespeichert, so dass eine Schwachstelle einheitlich in mehreren Patterns verwendet werden kann. In den Abbildungen 1 und 2 ist das z.B. „Rollen- und Rechtekonzept nicht ausreichend“. Bei Maßnahmen wird im Patternpool gespeichert, bei welchen Schwachstellen sie typischerweise verwendet werden.

4 Toolgestützte Assessments

4.1 Assessment auf Basis von Patterns mit mobilem Endgerät

Um Assessments durchzuführen, wird der gesamte Patternpool geordnet nach Ansprechpartnern, wie Geschäftsführung, Personalabteilung oder IT-Leitung und nach Bereichen (z.B. Verfahren) auf ein mobiles Engerät, beispielsweise ein Tablet, übertragen. Eine Übersicht zu der gesamten Architektur des IT-Services „Datenschutz-Cloud“ finden Sie in Abbildung 7. Der mobile Client zur Unterstützung von Assessments wird dort auch als Frontend bezeichnet.

Nach Auswahl des Ansprechpartners, des Bereichs und eines konkreten Patterns, kann

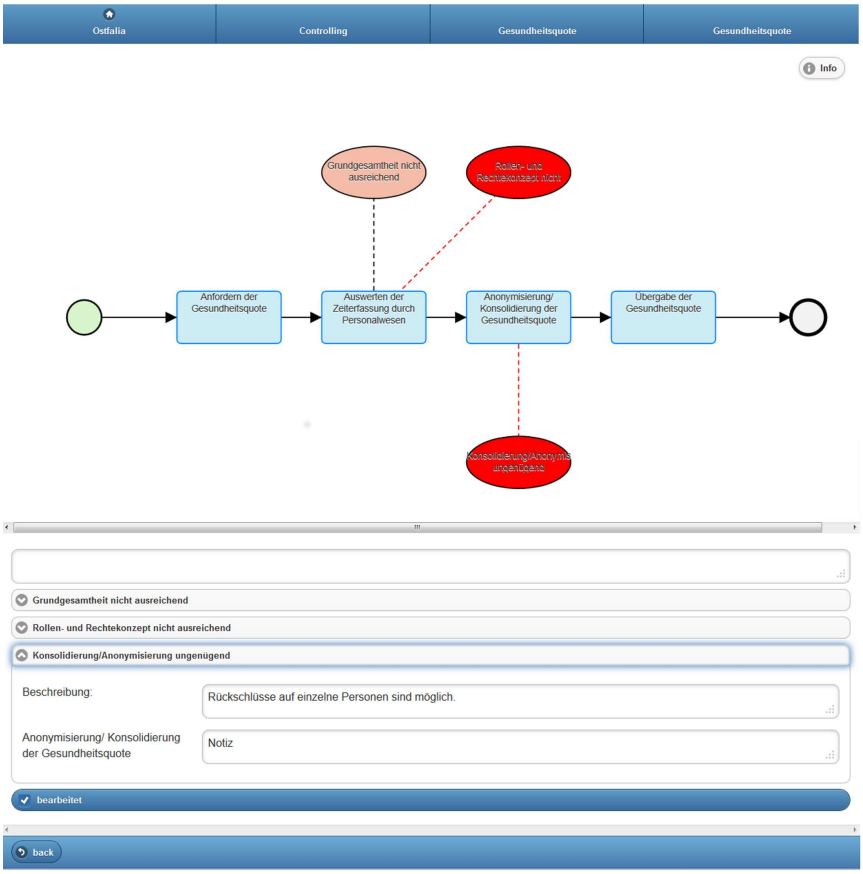

Abbildung 4: Pattern zum Verfahren „Gesundheitsquote“

man innerhalb des Patterns Schwachstellen in Verbindung mit Aktivitäten als zutreffend markieren. Diese werden nun rot dargestellt und man kann sowohl zum Pattern allgemein, als auch zu jeder Schwachstelle verbunden mit einer Aktivität Notizen in einem separaten Notizfeld machen (siehe Abb. 4). Der mobile Client gibt den Gesprächspartnern einen Überblick, welche Bereiche bereits bearbeitet wurden und welche Bereiche Schwachstellen enthalten und bietet damit einen roten Faden im Gespräch in Verbindung mit einer visuellen Unterstützung an, um Assessments vergleichbar durchzuführen.

4.2 Ergänzen von Maßnahmen zu Schwachstellen im Backend

Das Ergebnis des Assessments stellt den Ist-Zustand des Unternehmens aus datenschutzrechtlicher Sicht dar. Es besteht aus den verwendeten Patterns, die Verfahren im Unternehmen beschreiben oder bei denen technisch-organisatorische Maßnahmen geprüft wurden.

Zusätzlich wird gespeichert, wo Schwachstellen bei einem Pattern und einer Aktivität im Pattern im Assessment identifiziert wurden. Sowohl zum Pattern, als auch einem konkreten Vorkommen einer Schwachstelle können ergänzende Notizen erfasst werden.

Da Schwachstellen, die mehrfach in Patterns vorkommen im Backend durch einheitliche Elemente repräsentiert werden, kann das Ergebnis im Überblick als ungerichteter Graph dargestellt werden, mit Knoten die Patterns oder Schwachstellen darstellen. Damit ermöglicht man dem Datenschutzbeauftragten einen Überblick über den Ist-Zustand.

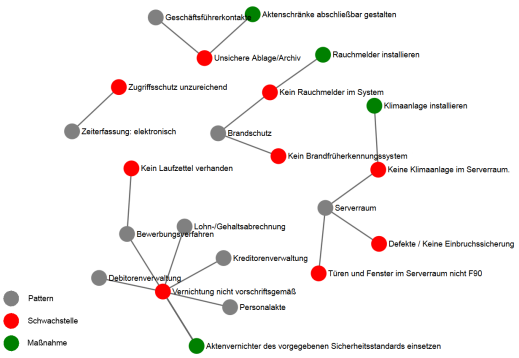

Abbildung 5: Strukturgraph - Ergebnis eines Assessments mit zugeordneten Maßnahmen

Über einen Web-Client im Backend des IT-Service können zu Schwachstellen Maßnahmen zugeordnet werden. Das Ergebnis des Assessments inklusive der zugeordneten Maßnahmen wird als *Strukturgraph* bezeichnet (siehe Abbildung 5). Dabei werden bei der Zuordnung von Maßnahmen Vorschläge angezeigt. Diese Vorschläge basieren darauf, dass bereits im Patternpool Maßnahmen angelegt und mit Schwachstellen verknüpft werden können. Die Reihenfolge der Anzeige basiert auf der Auswertung bereits abgeschlossener Strukturgraphen.

4.3 Regelmäßige Aktualisierung des Assessments

Durch die Flexibilität gerade von kleinen und mittleren Unternehmen, ist es notwendig in abgestimmten Intervallen das Assessment zu aktualisieren. Bei Assessments, die auf Fragebögen basieren, ist dieses aufwändig, da geprüft werden muss, auf welche der Fragen Änderungen im Unternehmen Auswirkungen haben.

Bei dem hier vorgestellten Ansatz von Assessments basierend auf Patterns, ist bereits ein Strukturgraph als Ergebnis eines vorangehenden Assessments vorhanden. Dieses Resultat des ersten Assessments oder der letzten Aktualisierung kann als Basis zusammen mit einer aktuellen Version des Patternpools auf den mobilen Client geladen werden. Nun kann ausgehend von den Patterns mit den Ansprechpartnern geklärt werden, in welchen Bereichen sich Änderungen oder Ergänzungen ergeben. Auch beim anschließenden Zuordnen von Maßnahmen kann auf den letzten Strukturgraphen zurückgegriffen werden, um einen Überblick über Änderungen zu gewinnen und Maßnahmen anzupassen.

5 Erstellen von Patterns im Patternpool

Der Patternpool kann über einen Web-Client im Backend ergänzt werden. Dadurch ist eine flexible Anpassung an neue Technologien oder neue Verfahren jederzeit möglich. Dazu können Schwachstellen und Maßnahmen direkt über einen Web-Client eingegeben und verknüpft werden. Die Erstellung von Patterns ist über einen Patterneditor möglich. Bei der Zuordnung von Schwachstellen kann ausschließlich auf im Patternpool bereits hinterlegte Schwachstellen zurückgegriffen werden. In Abbildung 6 wird der Patterneditor dargestellt.

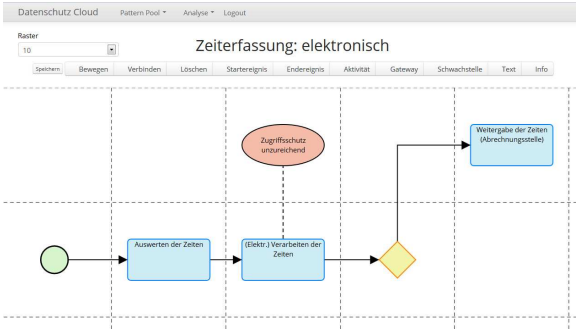

Abbildung 6: Erstellen von Patterns mit Patterneditor

6 Architektur des Gesamtsystems

Die Durchführung von Assessments und die Erstellung von Patterns werden wie folgt im Zusammenhang der gesamten Architektur realisiert: Zunächst kann mittels eines Web-Clients im Backend der Patternpool um Schwachstellen, Maßnahmen und Patterns ergänzt werden. Zur Durchführung von Assessments muss zunächst für das zu untersuchende Unternehmen ein Mandant im Backend erzeugt werden, falls das noch nicht geschehen ist. Dann wird der Patternpool auf den mobilen Client zur Durchführung des Assessments geladen. Anschließend an das Assessment, werden die Ergebnisse verknüpft an den Mandanten ins Backend geladen. Der mobile Client ist als HTML5-App realisiert, um einen plattformübergreifenden Einsatz zu ermöglichen.

Im Backend können zum Strukturgraphen Maßnahmen hinzugefügt werden. Um die Informationen bzgl. der Zuordnung von Maßnahmen als Hinweis für weitere Assessments nutzen zu können, werden aus dem Strukturgraphen sogenannte *Analysegraphen* extrahiert, die möglichst weitgehende Informationen zu der Situation erlauben sollen, in der eine Maßnahme angewendet wurde, ohne Rückschlüsse auf das Unternehmens zu ermöglichen, zu dem der Strukturgraph erhoben wurde.

Dazu werden aus dem Strukturgraphen Teilgraphen isoliert, die jeweils aus einer Schwachstelle mit allen Patterns und Aktivitäten gehören, in denen die Schwachstelle auftrat. Ein

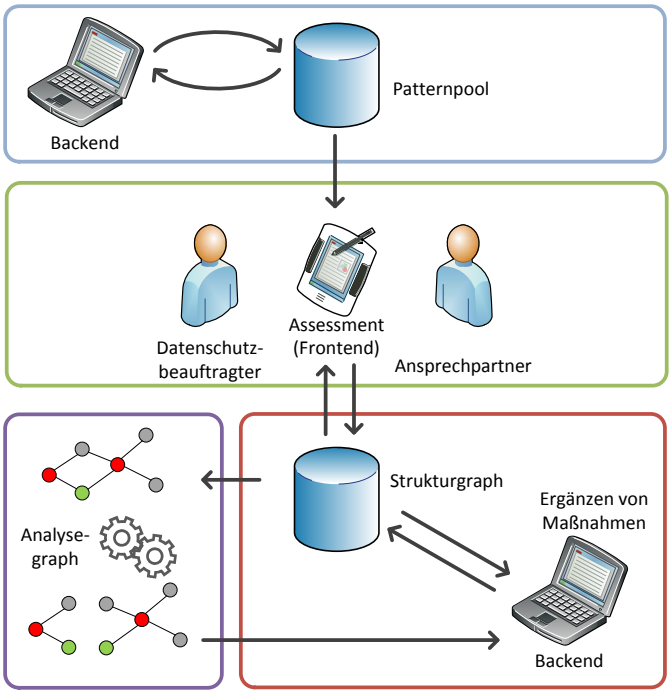

Abbildung 7: Übersicht IT Service Datenschutz-Cloud

Tupel bestehend aus Pattern, Aktivität, Schwachstelle und zugeordneter Maßnahme wird als *Kante* im Strukturgraph oder Analysegraph bezeichnet. Damit besteht ein Analysegraph aus einer Schwachstelle zusammen mit allen Kanten eines Strukturgraphen, in denen die Schwachstelle vorkommt.

Bei der Zuordnung von Maßnahmen zu Schwachstellen in einem neuen Strukturgraphen, werden nun die prinzipiell möglichen Maßnahmen gemäß eines Vergleichs der Umgebung der Schwachstelle im Strukturgraphen mit den Analysegraphen sortiert dargestellt. Dazu wurde ein Ähnlichkeitsmaß auf Analysegraphen definiert und ein darauf basierendes Ranking abgeleitet. Da Analysegraphen keinen Rückschluss auf andere Mandanten ermöglichen, können für das Ranking alle vorhandenen Analysegraphen verwendet werden. Faktoren die dabei eingehen, sind die Ähnlichkeit eines Analysegraphen mit der betrachteten Situation und das Entstehungsdatum des Analysegraphen. Bei der Aktualisierung von bestehenden Assessments, wird nun neben dem aktuellen Patternpool auch der bestehende Strukturgraph auf den mobilen Client geladen. Als Ergebnis wird jeweils ein aktueller Strukturgraph erzeugt, der zur Ergänzung von Maßnahmen und zur Archivierung ins Backend geladen wird.

7 Status und Abgrenzung

Der IT-Service, der im Projekt Datenschutz-Cloud entwickelt wurde, hat derzeit den Status eines Prototypen. Dieser Prototyp wurde von den Autoren anhand von abgeschlossenen Assessments evaluiert. Außerdem wurde besonders der mobile Client mehrfach in der Praxis eingesetzt und hat sich dort bereits bewährt. Dabei hat sich gezeigt, dass die gewählte Vorgehensweise die Zusammenarbeit und den Wissensaufbau zwischen Datenschutzbeauftragten mit stärker juristisch und technisch ausgeprägten Kompetenzen und damit qualitätsgesichertes Arbeiten in Teams fördert.

Der Aufbau der Patterns im Patternpool erfolgt durch den Industriepartner im Projekt nach Bedarf, um möglichst jeweils eine zeitnahe Erprobung von Patterns zu ermöglichen. Dabei wurden bisher Unternehmen untersucht, deren Geschäftsbeziehungen durch B2B (Business-to-Business) Geschäftsmodelle geprägt sind. Deshalb wurde bisher noch keine ausführliche Modellierung von Betroffenheitsrechten vorgenommen.

Aspekte, die besonders im Umgang mit personenbezogenen Daten von Kunden bei B2C (Business-to-Customer) kritisch sind und in dem hier vorgestellten Ansatz noch evaluiert werden müssen, sind z.B. die Zweckbindung mit verschiedenen Zugriffsrechten, Protokollierung auch von lesenden Zugriffen und die Klärung des Zugriffs auf Logs und Protokoll-Dateien. Hier lassen sich die Anforderungen der Betroffenen gut mithilfe von Datenschutz-Schutzzielen modellieren [BM12], [Pro12]. Dabei sollte im Weiteren evaluiert werden, wie sich Konflikte zwischen den Schutzzielen, wie z.B. zwischen Transparenz und Vertraulichkeit bei Zugriffen auf Logs und Protokolldateien, mittels Patterns modellieren lassen. Außerdem muss geklärt werden, inwieweit Schwachstellen, die sich aus der Anwendung von Maßnahmen ergeben, in diesem Ansatz darstellbar sind.

8 Zusammenfassung und Ausblick

Durch die Verwendung von Patterns als Basis von Assessments wird transparentes und qualitätsgesichertes Arbeiten im Bereich des Datenschutzes erleichtert. Datenschutzbeauftragte erhalten eine Unterstützung durch einen IT-Service, der auf ihrer bestehenden Fachkunde aufbaut.

Im nächsten Schritt soll der Patternpool weiter ausgebaut werden, um den Bereich B2C und branchenspezifische Verfahren stärker abzudecken und die in Kapitel 7 adressierten Punkte zu evaluieren. Außerdem sollen in einer Trainigsphase weitere Assessments durchgeführt werden, um die Struktur der Analysegraphen und das darauf basierende Ranking von Maßnahmen zu optimieren.

Danksagung: Dieses Vorhaben wird aus den Mitteln des Bundeswirtschaftsministeriums im Rahmen des Zentralen Innovationsprogramms Mittelstand (ZIM) unter den Förderkennzeichen KF3081801KM2 und KF2842903KM2 gefördert.

Literatur

[AIS77] Christopher Alexander, Sara Ishikawa und Murray Silverstein. A Pattern Language: Towns, Buildings, Construction (Center for Environmental Structure Series). 1977.

[BDS] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist. http://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html.

[Biz07] Johann Bizer. Sieben Goldene Regeln des Datenschutzes. *Datenschutz und Datensicherheit-DuD*, 31(5):350–356, 2007.

[BM12] Kirsten Bock und Sebastian Meissner. Datenschutz-Schutzziele im Recht. *Datenschutz und Datensicherheit-DuD*, 36(6):425–431, 2012.

[Bun13] Bundesamt für Sicherheit in der Informationstechnik (BSI). IT-Grundschutz-Kataloge, 2013. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/kataloge.html.

[Bus11] Business Process Model and Notation (BPMN). Version 2.0. *Object Management Group specification*, 2011.

[DG12] Nick Doty und Mohit Gupta. Privacy Patterns, 2012. http://privacypatterns.org/.

[fISB11] Federal Office for Information Security (BSI). Privacy Impact Assessment Guideline for RFID Applications, 2011.

[GHJV94] Erich Gamma, Richard Helm, Ralph Johnson und John Vlissides. *Design patterns: elements of reusable object-oriented software*. Pearson Education, 1994.

[Gru13] Michael Gruber. ISIS12 - Informationssicherheit für mittelständische Unternehmen. In *D-A-C-H Security 2013, Nürnberg*, Seiten 275 – 282. syssec, 2013.

[HWP+13] Thorsten Humberg, Christian Wessel, Daniel Poggenpohl, Sven Wenzel, Thomas Ruhroth und Jan Jürjens. Ontology-Based Analysis of Compliance and Regulatory Requirements of Business Processes. In *Proceedings of the 3rd International Conference on Cloud Computing and Services Science (Closer 2013)*, Seiten 553–561. SciTePress, 2013.

[ISO13] ISO/IEC. ISO/IEC 27001 - Information technology - Security techniques - Information security management systems - Requirements, 2013.

[LT12] Patrick Lundevall und Tommy Tranvik. Was sind personenbezogene Daten? Die Kontroverse um IP-Adressen. *Zeitschrift für Datenschutz (ZD)*, 03004, 2012.

[Off09] Information Commissioners Office. Privacy Impact Assessment Handbook, 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html.

[Pro12] Thomas Probst. Generische Schutzmaßnahmen für Datenschutz-Schutzziele. *Datenschutz und Datensicherheit*, 36(6):439–444, 2012.

[WDH12] David Wright und Paul De Hert. *Introduction to privacy impact assessment*. Springer, 2012.

[YWM08] Nobukazu Yoshioka, Hironori Washizaki und Katsuhisa Maruyama. A survey on security patterns. *Progress in Informatics*, 5(5):35–47, 2008.