Security-Management-as-a-Service für die öffentliche Verwaltung

Andreas Heinemann · Fabian Kern · Steffen Lange
Marian Margraf · Florian Otterbein

Hochschule Darmstadt
{andreas.heinemann | fabian.kern | steffen.lange
marian.margraf | florian.otterbein}@h-da.de

Zusammenfassung

Die vorliegende Arbeit stellt einen Ansatz vor, der kommunale Behörden bei der Etablierung eines ganzheitlichen IT-Sicherheitsprozesses und dessen Aufrechterhaltung im laufenden Betrieb unterstützt. Die wesentliche Idee besteht darin, derzeit umgesetzte organisatorische Sicherheitsmaßnahmen in Technische umzuwandeln, die wiederum durch einen zentralen Dienst ausgelagert werden können. Der zur Verfügung gestellte, zentrale Dienst soll die Kommune ebenfalls bei der Etablierung eines Informationssicherheitsmanagementsystems unterstützen. Um die Anforderungen an einen solchen zentralen Dienst formulieren zu können, wurden die IT-Infrastrukturen in verschiedenen kommunalen Bürgerämtern untersucht. Des Weiteren wurden Mitarbeiter befragt und bei der Durchführung ihrer Aufgaben beobachtet. Basierend auf diesen Untersuchungen wurden Hauptprobleme, die zu Sicherheitsvorfällen führen können, erhoben und zusammengefasst. Darauf aufbauend wird ein erster Lösungsvorschlag für die Konzeption und Einbindung des zentralen Dienstes diskutiert.

1 Einleitung

Die öffentliche Verwaltung ist eine der kritischen Infrastrukturen unseres Landes, siehe [dI11]. Ca. 5500 kommunale Bürgerämter sind mit Aufgaben rund um das Pass-, Personalausweis- und Meldewesen betraut und müssen u.a. IT-gestützt physische und elektronische Identitätsnachweise sicher und zuverlässig verwalten. Der IT-Sicherheit kommt deshalb eine besondere Bedeutung zu.

Die Etablierung und Beurteilung von IT-Sicherheit erfordert ein hohes Maß an Expertenwissen. IT-Sicherheit wird nicht durch einzelne ausgewählte Schutzmaßnahmen erreicht, sondern ist vielmehr ein ganzheitlicher Prozess, der in der Regel unter Nutzung eines sogenannten Informationssicherheitsmanagementsystems (ISMS) umgesetzt wird. Dies ist in der Regel mit den in kommunalen Institutionen vorhanden Ressourcen nicht zu leisten. Die stetig wachsende Komplexität von IT-Systemen und die daraus resultierenden steigenden Anforderungen an ihre IT-Sicherheit werden das Problem zukünftig noch verschärfen. Die regelmäßigen Berichte des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit zeigen, dass die Bedrohungslage in unserem Land immer mehr zunimmt, siehe [Bun15].

Eine weitere Herausforderung besteht darin, die Auswahl der Schutzmaßnahmen an die Bedürfnisse, Kenntnisse und Fähigkeiten der Anwenderinnen und Anwender anzupassen. Nur wenn die Maßnahmen akzeptiert und in den Arbeitsalltag integriert werden, können sie auch greifen.

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 264-275.

Im vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekt Security-Management-as-a-Service (SecMaaS) werden neue Vorgehensmodelle und neue technische Konzepte entwickelt, die es ermöglichen sollen, IT-Sicherheitsprozesse für die kommunalen Bürgerämter zu beurteilen und zu etablieren. Diese Modelle und Konzepte sollen auch ohne fundierte Kenntnisse einfach umsetzbar sein und eine einfache Bedienung ermöglichen.

Der vorliegende Artikel stellt den in diesem Projekt adressierten Ansatz vor, den wir als *Security-Management-as-a-Service* bezeichnen (Abschnitt 3). Weiter werden relevante Vorarbeiten in Abschnitt 2, die zugrunde liegende Methodik in Abschnitt 4 sowie erste Ergebnisse in den Abschnitten 5 und 6 präsentiert.

2 Related Work

Ein Cloud-Service ist im Wesentlichen eine von einem externen Dienstleister zur Verfügung gestellte IT-Infrastruktur, die es bspw. Unternehmen oder Organisationen erlaubt, bestimmte IT-Dienstleistungen auszulagern. Das National Institute of Standards and Technology (NIST) unterscheidet in [PT11] vier Bereitstellungsmodelle (Private-Cloud, Community-Cloud, Public-Cloud und Hybrid-Cloud) und drei Servicemodelle.

Eine *Private-Cloud* ist eine IT-Infrastuktur, die exklusiv einem Cloud-Nutzer zur Verfügung steht, während eine *Community-Cloud* von einem eingeschränkten Kreis verwendet wird. Im Unterschied zu diesen beiden Bereitstellungsmodellen ist eine *Public-Cloud* offen über das Internet zugänglich und kann von jedermann genutzt werden. Eine *Hybrid-Cloud* ist eine Mischform dieser ersten drei Bereitstellungsmodelle.

Wird vom Cloud-Anbieter nur die IT-Infrastruktur, d.h. Hardwareressourcen (Rechenleistung und Speicherplatz), bereitgestellt, heißt der angebotene Service Infrastructure-as-a-Service (IaaS). Stellt der Cloud-Anbieter zusätzliche IT-Dienstleistungen, bspw. die Nutzung von Entwicklungs- und Laufzeitumgebungen, bereit und unterhält diese, wird das Service Plattform-as-a-Service (PaaS) genannt. Im Unterschied dazu heißt der Service Software-as-a-Service (SaaS), wenn die zur Verfügung gestellte IT-Infrastruktur nur verwendet werden kann, um vom Cloud-Anbieter bereitgestellte und unterhaltene Anwendungssoftware zu nutzen.

Da Cloud-Services eine ganze Reihe von Diensten bündeln, sind sie ein attraktives Ziel für Angreifer. Die meisten Arbeiten im Bereich Cloud-Sicherheit befassen sich deshalb mit deren Absicherung, siehe bspw. [MKL09] und [Bun16], sowie dem IT-Sicherheitsmanagementprozess für Cloud-Services, siehe u.a. [KC12] und [DRS10]. Notwendige Schutzmaßnahmen zur Umsetzung der klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sind damit auf die vom Cloud-Anbieter bereitgestellte IT-Infrastruktur, die darauf laufenden Anwendungen, sowie die von diesen Anwendungen zu verarbeitenden und zu verwaltenden Daten beschränkt. Die lokale IT-Infrastruktur der Cloud-Nutzer bleibt weitestgehend unberücksichtigt.

Neben dem Thema Cloud-Sicherheit gibt es Ansätze, Cloud-Services im Sinne von SaaS bzw. PaaS zu konzipieren und umzusetzen, die es den Cloud-Nutzern erlauben, einzelne technische und organisatorische Sicherheitsmaßnahmen, wie bspw. die Verschlüsselung von E-Mails oder ein Identitätsmanagement, siehe [FHMS12] und [DRS10], auszulagern. Solcherart Cloud-Services werden in der Regel Security-as-a-Service (SecaaS) genannt. Der Begriff SecaaS wird nicht einheitlich verwendet. Angebote externer Dienstleister, das IT-Sicherheitsmanagement für ein Unternehmen zu übernehmen, werden mitunter auch SecaaS genannt.

Security-Management-as-a-Services (SecMaaS) bezeichnet einen Cloud-Service, der den Cloud-

Nutzer bei der Etablierung, Umsetzung, Bewertung und Aufrechterhaltung eines ganzheitlichen IT-Sicherheitsmanagementprozesses unterstützt. Die zur Umsetzung erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen können – analog wie bei SecaaS – ausgelagert werden, d.h. SecaaS-Angebote sind ein essentieller Bestandteil eines SecMaaS.

3 Security-Management-as-a-Service

Ein ISMS ist eine Sammlung von Vorgehensweisen, Vorschriften und Schutzmaßnahmen, um einen IT-Sicherheitsprozess zu etablieren und im laufenden Betrieb aufrechtzuerhalten. Vorgehensmodelle für die Umsetzung eines ISMS sind z.B. die Normenreihe ISO 2700x und der IT-Grundschutz des BSI. Zentraler Bestandteil eines ISMS ist die Erarbeitung und Umsetzung eines IT-Sicherheitskonzepts.

Bei der Etablierung eines ISMS wird in der Regel wie folgt vorgegangen: Zunächst werden in der IT-Strukturanalyse alle Bestandteile des IT-Verbunds[1] der Institution beschrieben. In einer Schutzbedarfsanalyse wird anhand von möglichen Schadensszenarien der Schutzbedarf der Daten, IT-Systeme (inkl. Netze) und Räumlichkeiten ermittelt. Die Gefährdungsanalyse ermittelt mögliche Gefährdungen, die Schäden verursachen können, die in der Risikoanalyse an Hand der Eintrittswahrscheinlichkeit und den möglichen Schäden klassifiziert werden. Anhand der Risikoanalyse werden nun Schutzmaßnahmen für jede Gefährdung ausgewählt. Zum Abschluss wird mittels einer (extern oder intern) durchgeführten Evaluierung überprüft, ob die ausgewählten Schutzmaßnahmen wirksam und ausreichend sind, um den IT-Verbund in seiner Gesamtheit zu schützen.

Damit wird IT-Sicherheit entsprechend der momentanen Gefährdungslage umgesetzt. Bei neuen Gefährdungen, einer Veränderung von Risiken oder auch Lücken, die im Rahmen der Evaluierung nicht bemerkt wurden, muss das IT-Sicherheitskonzept entsprechend angepasst werden.

Wie bereits in der Einleitung beschrieben, beschäftigen wir uns in dieser Arbeit mit der Absicherung der IT-Infrastrukturen in kommunalen Bürgerämtern. Viele Geschäftsprozesse dieser Institutionen, wie z.B. das Pass-, Personal- und Meldewesen, sind durch bundesgesetzliche Regelungen vorgeschrieben, die übrigen durch Landesgesetze, die sich aber in der Regel in ihren Auswirkungen in Hinblick auf die eingesetzte IT-Infrastruktur nicht allzu stark unterscheiden. In der Folge sind die in kommunalen Bürgerämtern vorhandenen IT-Infrastrukturen sehr ähnlich. Dies betrifft insbesondere die verwendeten IT-Komponenten (z.B. Computer, Drucker, Fingerabdruckscanner, Pass-, Personal- und Melderegister) und die verwendeten Netze insb. die Schnittstellen nach außen (z.B. zur Bundesdruckerei bzw. zu hoheitlichen Stellen).

Ein IT-Sicherheitskonzept kann also gebündelt für mehrere kommunale Behörden erstellt werden. Ähnliches gilt für die Evaluierung der Schutzmaßnahmen und die Aufrechterhaltung im laufenden Betrieb. Eine Änderung der Gefährdungslage betrifft alle kommunalen Behörden.

Um die Komplexität des IT-Sicherheitsmanagementprozesses zu reduzieren, ist es vorteilhaft, auch technische und organisatorische Maßnahmen zu bündeln und für diese Bedarfsträger zentral in einer Cloud zur Verfügung zu stellen. Offensichtlich lassen sich aber nicht alle Schutzmaßnahmen durch einen zentralen Cloud-Service umsetzen. So müssen Maßnahmen, wie z.B.

[1] Der BSI-Grundschutz versteht unter einem IT-Verbund die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.

der Schutz der Räumlichkeiten oder die Mitarbeiterverwaltung, in den Behörden umgesetzt werden.

Ziel soll es sein, einen zentralen Cloud-Service so zu gestalten, dass dieser es den kommunalen Bürgerämtern ermöglicht, auch ohne fundierte Kenntnisse ein ISMS zu etablieren, komplexe Schutzmaßnahmen (sowohl technische als auch organisatorische) auszulagern und Unterstützung bei der Beurteilung, Auswahl und Umsetzung der dezentral im Bürgeramt verbleibenden Sicherheitsmaßnahmen zu bieten. Dabei soll sichergestellt werden, dass die zentralen und dezentralen Schutzmaßnahmen so aufeinander abgestimmt sind, dass ein angemessen hohes Schutzniveau für die Gesamtlösung erreicht wird. Einen solchen Cloud-Service bezeichnen wir als *SecMaaS*.

4 Vorgehen

Die von uns verwendete Methodik lehnt sich an den im Hassno-Plattner-Institut in Potsdam und der Stanford University entwickelten *Design Thinking*-Prozess an. Bei diesem sechsstufigen Prozess (Abbildung 1) wird der Benutzer von Anfang an mit einbezogen [PMW11].

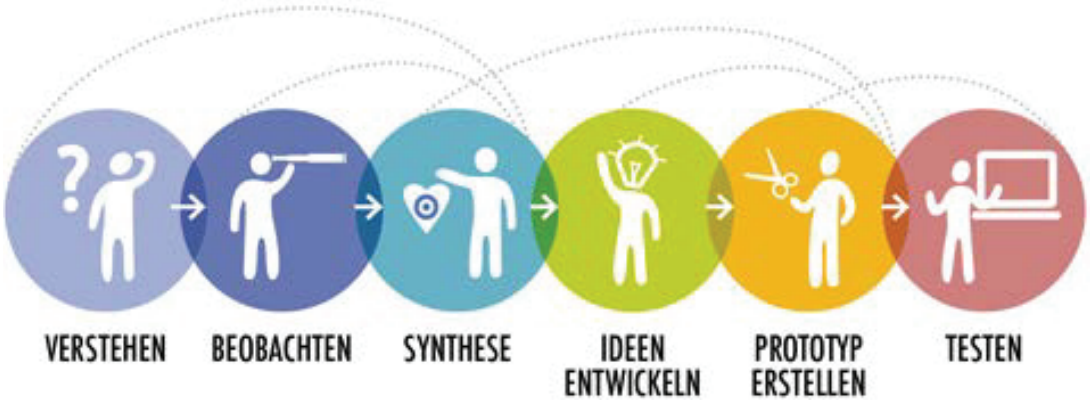

Abb. 1: Der *"Design-Thinking"*-Prozess als iteratives Vorgehensmodell, siehe [Rus16].

Basierend auf einer konkreten Fragestellung (im SecMaaS-Projekt: Wie kann die IT-Sicherheit in kommunalen Behörden auf ein notwendiges Sicherheitsniveau gehoben werden?) werden Informationen über das Thema zusammengetragen und konkrete Probleme ermittelt und ein Lösungsvorschlag erarbeitet und evaluiert. Neben der Literaturrecherche kann die Beobachtung und Befragung der Anwender hilfreich sein. Mit Hilfe von *Job Shadowing*, dem Beobachten des Anwenders bei der Arbeit und qualitativen Nutzerinterviews kann Empathie aufgebaut werden [MLM15], sodass es möglich ist, sich in die Rolle des Anwenders hineinzuversetzen. Durch Ausprobieren und Anwenden können die Geschäftsprozesse selbst erfahren werden und innovative und kreative Lösungen dadurch einfacher gefunden werden, als durch analytisches Nachdenken [PMW11]. Die gesammelten Informationen werden anschließend gebündelt und deren Essenz extrahiert.

Im SecMaaS-Projekt stellten sich die Untersuchungsphasen wie folgt dar:

- In Phase 1 (Verstehen) wurde zunächst, ausgehend von den in einer typischen kommunalen Behörde durchgeführten Geschäftsprozessen, eine IT-Struktur- und Schutzbedarfsanalyse in Anlehnung an den IT-Grundschutz des BSI durchgeführt. Anschließend wurden die Bedürfnisse, Kenntnisse und Fähigkeiten der verantwortlichen Mitarbeiter anhand

qualitativer Tiefeninterviews ermittelt und typische Rollen definiert. Einige Ergebnisse dieser Untersuchung finden sich in den Abschnitten 5.1 und **??**.

- In Phase 2 (Beobachten) wurden die Sacharbeiter der Behörde bei der Durchführung ihrer Aufgaben beobachtet. Im Anschluss wurden die Beobachtungen im Rahmen von qualitativen Tiefeninterviews verfeinert. Einige Ergebnisse dieser Untersuchung finden sich in Abschnitt **??**.
- In Phase 3 (Synthese) wurden, basierend auf den Ergebnissen aus den Phasen 1 und 2 die Hauptprobleme hinsichtlich der oben formulierten Fragestellung sowie die Gründe hierfür ermittelt und geeignet zusammengefasst, siehe Abschnitt 5.3.
- In Phase 4 (Ideen entwickeln) wurden Lösungen entwickelt, die zuvor aufgedeckten Probleme zu beheben, siehe Abschnitt 6.

In den nächsten Schritten werden die entwickelten Lösungen in Form von rudimentären, nichtfunktionalen Prototypen für die Zielgruppen umgesetzt, die wiederum Feedback für das weitere Vorgehen geben werden. Die entsprechenden Arbeiten sind noch nicht abgeschlossen.

Insgesamt wurden 13 Sachbearbeiter, sechs Mitarbeiter der IT-Abteilung und zwei Behördenleiter in vier unterschiedlichen kommunalen Behörden befragt und zum Teil beobachtet. Die Untersuchungen wurden von einer Gruppe von sieben Mitarbeitern der Hochschule Darmstadt und der Freien Universität durchgeführt.

5 Ergebnisse

Im Folgenden werden die Ergebnisse der Untersuchungen in Phase 1-3 kurz zusammengefasst. Ergebnisse von Phase 4 finden sich in Abschnitt 6.

5.1 IT-Infrastruktur- und Schutzbedarfsanalyse

Auf Details der Analyse wird aus Platzgründen an dieser Stelle verzichtet. Wie aber bereits in Abschnitt 3 beschrieben, sind die Geschäftsprozesse kommunaler Behörden sehr ähnlich, so dass sich der Schutzbedarf für verarbeitende Daten und verwendete IT-Komponenten und Netze auch für Behörden in unterschiedlichen Bundesländern nicht unterscheidet. Für die verwendete IT-Infrastruktur gibt es im Wesentlichen zwei Ausprägungen:

1. Behörden verwalten ihre IT-Infrastruktur eigenständig. Die Anwendungssoftware für die umzusetzenden Geschäftsprozesse (Fachverfahren) wird von externen Dienstleistern erworben.
2. Behörden lagern Teile der IT-Infrastruktur an IT-Dienstleister aus, bspw. Melde-, Personalausweis- und Reisepassregister, aber auch die gesamte Anwendungssoftware (Fachverfahren).

In keiner der von uns untersuchten Behörden fanden wir ein vollständig umgesetztes ISMS vor. Selbst in den Behörden, die ihre IT-Infrastruktur nahezu vollständig auslagern, fand keine ganzheitliche Betrachtung der IT-Sicherheitsmaßnahmen statt.

5.2 Befragung der Mitarbeiter

Nach IT-Grundschutz des BSI sind personelle Maßnahmen wesentlich für die Etablierung eines IT-Sicherheitsmanagementprozesses. Zur Beurteilung und Umsetzung personeller Maßnahmen

sind also sowohl die fachliche Qualifikation der Mitarbeiter als auch die Motivation, sich in Themen der IT-Sicherheit einzuarbeiten und die Bereitschaft, aktiv bei der Umsetzung von technischen und organisatorischen Sicherheitsmaßnahmen mitzuwirken, wichtige Voraussetzungen. Weiter ist nach IT-Grundschutz IT-Sicherheit eine Querschnittsaufgabe, muss also von den Vorgesetzten im besonderen Maße unterstützt werden. Daher wurden in der ersten Phase der Untersuchung die Bedürfnisse, Kenntnisse und Fähigkeiten, der in den Rollen Sachbearbeiter, IT-Personal und Behördenleiter agierenden Behördenmitarbeitern, ermittelt. Diese lassen sich wie folgt beschreiben:

Die **Sachbearbeiter** der untersuchten Behörden kommen während der Ausbildung nicht mit den Themen IT-Sicherheit und Datenschutz in Berührung. Die meisten befragten Sachbearbeiter (9 von 13) sind sich der Folgen von mangelhafter Umsetzung von IT-Sicherheit bewusst, informieren sich regelmäßig über aktuelle Gefährdungen und nutzen dieses Wissen im privaten, jedoch nicht im beruflichen Umfeld. Sie blenden das Thema IT-Sicherheit im Arbeitsumfeld weitestgehend aus und sind in ihrem Verständnis ausschließlich dafür zuständig, ihre eigentlichen Arbeitsaufgaben zu erfüllen.

Das **IT-Personal** der besuchten Behörden unterscheidet sich in Bezug auf ihren Ausbildungsweg: einige haben eine technische Ausbildung durchlaufen (z.B. Fachinformatik), andere haben eine Verwaltungsausbildung absolviert und sich in ihrer Freizeit im IT-Bereich weitergebildet. Die Motivation, sich in Themen der IT-Sicherheit einzuarbeiten und sich in diesem Bereich weiterzubilden, ist in beiden Gruppen groß. Problematisch wird vom IT-Personal gesehen, dass in den jeweiligen Behörden eine einheitliche IT-Sicherheitsrichtlinie fehlt. Ebenfalls ist es schwer zu beurteilen, ob durch die von ihnen veranlassten Sicherheitsmaßnahmen ein in der Gesamtheit angemessenes Schutzniveau erreicht wird. Das IT-Personal kennt das dem IT-Grundschutz des BSI zugrunde liegende Vorgehen, kann es aber aufgrund seiner Komplexität und der beschränkten Zeitressourcen nicht auf die bestehende IT-Infrastruktur anwenden. Es ist daran interessiert, dass Sicherheitsmaßnahmen umgesetzt werden, die den agierenden Behördenmitarbeitern die Durchführung ihrer eigentlichen Arbeitsaufgaben nicht unnötig verkompliziert.

Die **Behördenleiter** der untersuchten Behörden haben in der Regel keinen technischen Hintergrund, sondern Verwaltungswissenschaften studiert. Das Interesse für den IT-Bereich ihrer Behörde ist eher gering. In der Folge schätzen sie die Gefährdungen und die damit einhergehenden Risiken als deutlich zu gering ein. Die Umsetzung von Sicherheitsmaßnahmen wird von ihnen kritisch hinterfragt, da die Reduzierung der Kosten im Mittelpunkt steht. Diese falsche Sichtweise ist besonders kritisch, da IT-Sicherheit nach IT-Grundschutz eine Querschnittsaufgabe ist und somit insb. die Unterstützung der Hausleitung benötigt, um erfolgreich umgesetzt werden zu können.

5.3 IST-Situation bzgl. IT-Sicherheit

Im Rahmen des Job Shadowing wurden 13 Sachbearbeiter in vier Behörden jeweils 40 Minuten begleitet. In dieser Zeit konnten einige Sicherheitsverstöße beobachtet werden:

- Der Rechner wurde nicht gesperrt, wenn der Arbeitsplatz kurz verlassen wurde.
- Bildschirme waren zum Teil so aufgestellt, dass personenbezogene Daten von anderen Kunden eingesehen werden konnten.
- Weitere Probleme ergaben sich aus den z.T. komplizierten Passwortregeln. Sachbearbeiter sind für eine Vielzahl von Fachverfahren zuständig. Die dafür eingesetzten Program-

me regeln die Zugriffsbeschränkungen selbständig, d.h. zur Authentifizierung benötigt der Sachbearbeiter separate Passwörter, die fachverfahrensspezifischen Passwortregeln genügen müssen (Einschränkungen in Bezug auf die Länge, die syntaktische Struktur und die zeitliche Gültigkeit von Passwörtern). Dadurch müssen sich Sachbearbeiter eine Reihe verschiedener Passwörter merken bzw. notieren.

In den anschließenden Gesprächen mit Sachbearbeitern wurden weitere Sicherheitsverstöße bekannt:

- In einer Behörde konnten alle Mitarbeiter alle Zugriffsrechte für verschiedene Fachverfahren selbst verändern.
- Anfragen von hoheitlichen Behörden (z.B. Polizei, Zollamt) zu Einträgen aus Registern wurden sowohl telefonisch als auch via E-Mail erteilt, ohne den Anfragenden zu authentisieren oder die Daten (bei E-Mailkommunikation) zu verschlüsseln.
- In zwei der untersuchten Behörden müssen Sachbearbeiter während persönlicher Kundenkontakte auch Telefonate annehmen, in denen personenbezogene Daten über das Telefon kommuniziert werden, so dass der Kunde vor Ort diese Daten mithören kann. Einige Sachbearbeiter arbeiten zudem parallel an beiden Vorgängen (Eingabe von Daten am Computer für Kunden vor Ort während des Telefonats), was ebenfalls zu Fehlern führen kann.

Auch die Interviews mit dem IT-Personal ergaben, dass weitere Sicherheitsverstöße vorgekommen sind:

- In einer der vier Behörden wurde bereits Schadsoftware über E-Mails eingeschleust.
- Sicherheitsmaßnahmen, wie z.B. die Sperrung von USB-Ports, mussten auf Verlangen der Vorgesetzten wieder aufgehoben werden.
- Die Erneuerung von Zertifikaten wurde in der Vergangenheit häufiger vergessen.

Gerade in Bezug auf das Zertifikatsmanagement ist insbesondere das Schutzziel Verfügbarkeit stark gefährdet. Behörden benötigen nach eigenen Aussagen bis zu zehn verschiedene Zertifikate, um ihre Aufgaben zu erledigen (z.B. Zertifikate für das Deutsche Verwaltungsdienstverzeichnis (DVDV), das Online Services Computer Interface (OSCI)[2], das Änderungsmanagement für die Online-Ausweisfunktion des Personalausweises (PIN-Änderung, Aktivierung und Deaktivierung, Adressänderung), den Antrags- und Bestätigungsprozess für hoheitliche Dokumente). Das Lifecycle-Management (Beantragung- bzw. Erneuerung, Nutzung, Sperrung) für diese Zertifikate unterscheidet sich zum Teil wesentlich. Gleiches gilt für die Sicherheitsvorgaben innerhalb der Public Key Infrastrukturen (PKI), in denen die Zertifikate ausgestellt werden.

5.4 Synthese

Es war zu beobachten, dass gerade gegen Sicherheitsmaßnahmen, die nicht technisch sondern organisatorisch umgesetzt werden müssen, verstoßen wird. Vor dem Hintergrund, dass die Sachbearbeiter nur eine geringe Motivation haben, sich mit IT-Sicherheitsmaßnahmen in ihrem Arbeitsumfeld zu beschäftigen, werden also Maßnahmen zur Sensibilisierung nur wenig Erfolg haben.

Eine weitere Erkenntnis ist, dass die Umsetzung von Schutzmaßnahmen häufig zu kompliziert

[2] Protokollstandard für die deutsche öffentliche Verwaltung.

oder nicht einheitlich ist (z.B. Passwortregeln, Zertifikatsmanagement) und daher zu Sicherheitsverstößen führt. Für einige Geschäftsprozesse existieren gar keine geeigneten Sicherheitsmaßnahmen (z.B. Kommunikation mit externen Behörden). Darüber hinaus sind die Rollen nicht klar definiert (Wer legt Schutzmaßnahmen fest? Wer darf Schutzmaßnahmen wieder aufheben? Wer verwaltet Zugriffsrechte?).

Im IT-Grundschutz werden insgesamt 46 unterschiedliche Rollen festgelegt (z.B. Administrator, Änderungsmanager, Anforderungsmanager, Leiter Entwicklung, IT-Betreuer, Sicherheitsbeauftragter, Verantwortliche für die Datensicherung). Diese Rollen müssen zwar personell nicht getrennt werden, allerdings zeigt sich schon aus den hier aufgeführten Rollen, dass eine hohe Expertise in unterschiedlichsten Bereichen innerhalb der kommunalen Bürgerämter vorhanden sein muss, um alle Aufgaben mit hoher Qualität umsetzen zu können. Zwar lagern alle der von uns untersuchten Behörden Teile ihrer Aufgaben aus, aber auch in diesem Fall muss in der Behörde entsprechendes Expertenwissen vorhanden sein, um die Qualität der Umsetzung der von den externen Dienstleistern übernommenen Aufgaben beurteilen zu können.

6 SecMaaS für Behörden

Aus der Synthese in Abschnitt 5.4 lassen sich mehrere Lösungsmöglichkeiten ableiten, die das IT-Sicherheitsniveau in kommunalen Behörden deutlich erhöhen können.

1. Entwicklung einheitlicher Sicherheitspolitiken, z.B. für das Lifecycle-Management für Zertifikate und Passwortregeln, die von allen IT-Dienstleistern (z.B. den Fachverfahrensentwicklern) umgesetzt werden müssen.
2. Umwandlung organisatorischer in technische Maßnahmen und Übernahme dieser durch einen externen Dienstleister.
3. Unterstützung der kommunalen Behörden bei der Umsetzung eines ISMS basierend auf 1. und 2.

Durch die Umwandlung organisatorischer in technische Maßnahmen und deren Auslagerung wird die Komplexität innerhalb der Behörde deutlich reduziert und das IT-Personal entlastet. Darüber hinaus können hierdurch auch einheitliche Sicherheitspolitiken besser umgesetzt werden. Insgesamt kann dies sowohl zu einer Erhöhung der Benutzbarkeit, als auch des Sicherheitsniveaus führen.

Zusätzlich sollen die Sicherheitspolitiken und übernommenen technischen Sicherheitsmaßnahmen hinsichtlich ihrer Wirksamkeit geeignet zertifiziert werden (z.B. nach IT-Grundschutz des BSI) damit auch die Beurteilung der Qualität der Umsetzung nicht in den Behörden verbleibt, sondern von akkreditierten Prüfstellen übernommen wird.

Basierend auf den durchgeführten Untersuchungen schlagen wir eine variable Gestaltung des IT-Verbundes vor, bei der einzelne Teile des IT-Verbundes inkl. der benötigten Schutzmaßnahmen ausgelagert werden. Hier greift der Ansatz des *Security-Management-as-a-Service*. Ausgelagerte Teile des Verbundes können mithilfe eines zentral organisierten ISMS abgesichert werden. Bei den verbleibenden Komponenten des IT-Verbundes zeigt sich, dass bei allen kommunalen Behörden eine sehr ähnliche IT-Struktur benötigt wird. Hier können wir die Analyse nach IT-Grundschutz des BSI vorwegnehmen, Maßnahmen so auswählen, dass sie einfach umsetzbar sind und die Verantwortlichen direkt mit einer vollständigen Liste umzusetzender Maßnahmen ausstatten.

Damit ergibt sich in der Gesamtheit ein vollständiges ISMS, welches Geschäftsprozesse dieser Behörden angemessen schützt. Der Grad der Auslagerung und somit der Komplexitätsgrad der verbleibenden IT-Landschaft wird dynamisch modelliert, wobei weitere Aspekte wie bspw. Kosten oder individuelles Know-How der einzelnen Bürgerämter berücksichtigt werden können.

Abbildung 2 illustriert die vorgeschlagene Lösung anhand von zwei fiktiven Behörden A und B. Behörde B lagert möglichst viele Komponenten und IT-Systeme aus und reduziert damit die noch vor Ort verbleibenden Schutzmaßnahmen. Behörde A hingegen lagert kaum Komponenten aus. Unsere Vorab-Analyse kann hier zumindest eine erschöpfende Liste aller lokal umzusetzenden Maßnahmen liefern und Handlungsempfehlungen geben, die in ein klassisches ISMS-Tool wie verinice[3] importiert werden können.

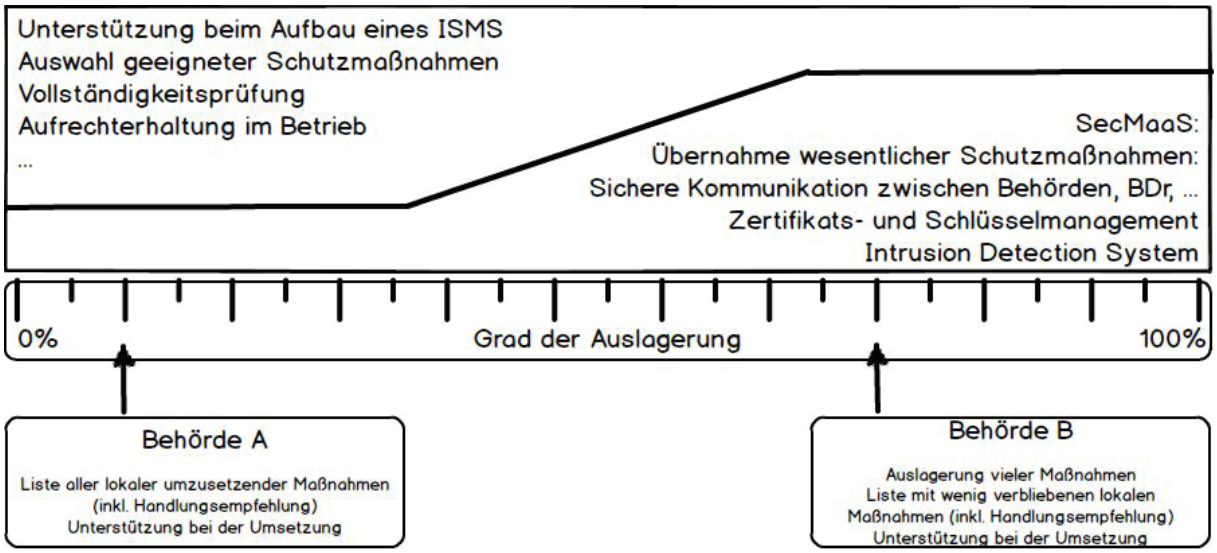

Abb. 2: Security Management as a Service – Lösungsvorschläge

Im Folgenden beschreiben wir einen Teil der Maßnahmen, die von einem externen Dienstleister übernommen werden können bzw. Maßnahmen, die derzeit in kommunalen Behörden zwar umgesetzt werden aber nicht wirksam sind (organisatorische Maßnahmen) ersetzen. Wir setzen dabei voraus, dass der externe Dienstleister vertrauenswürdig ist (festgestellt über eine geeignete Zertifizierung) und damit auch im Namen seines Kunden (einer kommunalen Behörde) agieren kann.

6.1 Zertifikatsmanagement

Wie bereits in Abschnitt 5.3 beschrieben, benötigen kommunale Behörden eine Reihe von Zertifikaten aus unterschiedlichen PKIs zur Erfüllung ihrer Aufgaben. Sowohl das Lifecycle-Management, als auch die Sicherheitsvorgaben innerhalb der PKIs unterscheiden sich.

Ein cloud-basiertes Zertifikatsmanagement kann die Beantragung, Sperrung, Wiederaufnahme und Erneuerung sowie die Konfiguration für die Behörde automatisieren und somit als unterstützende Sicherheitsmaßnahme dienen.

Dadurch können Ausfallzeiten aufgrund von falsch konfigurierten, widerrufenen oder abgelaufenen Zertifikaten vermieden und der Arbeitsaufwand für das IT-Personal verringert werden.

[3] http://verinice.org, Abruf am 8. April 2016

Teile des Zertifikatsmanagements müssen dabei in der Behörde verbleiben. So muss z.B. der Cloud-Service darüber informiert werden, wenn ein Mitarbeiter die Behörde verlässt oder Chipkarten, die die entsprechenden geheimen Schlüssel speichern, verloren gehen. Darüber werden die Behörden im Rahmen der oben genannten Handlungsempfehlungen informiert, so dass die umzusetzenden Sicherheitsmaßnahmen aufeinander abgestimmt sind und sich in der Gesamtheit ein angemessen hohes Sicherheitsniveau ergibt.

6.2 Passwortregeln und Intrusion Detection System

Wie bereits in Abschnitt 5.3 gesehen, benötigen Sachbearbeiter Passwörter für verschiedene Anwendungen mit unterschiedlichen Regeln (Länge, syntaktische Struktur, zeitliche Gültigkeit).

Zhang et al. haben in [ZMR10] gezeigt, dass Passwortregeln, bei denen ein häufiger Wechsel notwendig ist, nicht das IT-Sicherheitsniveau verbessern. Abgelaufene und neu gesetzte Passwörter sind häufig sehr ähnlich. Des Weiteren argumentieren die Autoren, dass unter Berücksichtigung der Usability sehr starke Passwörter nur dann sinnvoll sind, wenn der Account online verfügbar ist und über keinen Sperrmechanismus verfügt. Während unseren Untersuchungen in den Behörden beobachteten wir, dass komplizierte Passwörter im Klartext aufgeschrieben werden. Eine Studie von Yaacov Apfelbaum kam zu dem Ergebnis, dass eine zu strenge Passwortregel Ursache für aufgeschriebene Passwörter ist [Ape04].

Die von uns beobachteten Passwortregeln für verschiedene Anwendungen und die sich daraus ergebene Anzahl unterschiedlicher Passwörter führt also zu einem Verlust an Sicherheit. Mögliche Verbesserung ist die Umsetzung eines Single Sign-on Verfahrens, d.h. der Sachbearbeiter authentisiert sich nur an seinem Arbeitsplatzrechner und kann dann auf alle Dienste, für die er Berechtigungen hat, zugreifen. Begleitet werden sollte dieses Verfahren mit einem cloudbasierten Intrusion Detection System (IDS), das in der Lage ist, Angriffe, die versuchen Zugang zu den Rechnern zu erhalten, zu erkennen und in Verbindung mit einem Intrusion Prevention System auszusperren.

Da es in den von uns besuchten Behörden bereits zu Problemen mit Malware kam, die via E-Mail verteilt wurde, kann ein IDS mit geteilter Wissensbasis genutzt werden, um Schadsoftware zu erkennen. In der Datenbank können zusätzlich behördenspezifische Angriffsmuster enthalten sein, die regelmäßig aktualisiert werden. Mit solch einer Umsetzung können also nicht nur komplexe Passwortregeln ersetzt, sondern zusätzliche Sicherheitsmaßnahmen umgesetzt werden, die das Sicherheitsniveau insgesamt erhöhen.

6.3 Unterstützung beim IT-Sicherheitsmanagement

Der hier vorgestellte Ansatz Security-Management-as-a-Service bietet hinsichtlich der Umsetzung eines Informationssicherheitsmanagements eine Reihe von Vorteilen und Erleichterungen für die Behörden. Durch die technische und organisatorische Auslagerung von Maßnahmen in die Cloud kann für die lokal verbleibende IT der Behörde aufgrund der vorweggenommenen Struktur- und Risikoanalyse und Schutzbedarfsfeststellung sofort eine Liste mit den vor Ort umzusetzenden Sicherheitsmaßnahmen bereitgestellt werden. Diese Liste kann als Import für klassische ISMS-Werkzeuge wie verinice einem Benutzer leichtverständlich zur Verfügung gestellt werden.

Darüber hinaus bietet der zentrale Cloud-Service die Möglichkeit eines vereinfachten Monitorings der Bedrohungslage, z.B. auf Basis des im Abschnitt 6.2 beschriebenen Intrusion Detecti-

on Systems. Mithilfe dieser zentralen Erhebung kann dann unter Berücksichtigung des Wissens über den lokalen bzw. zentralen/ausgelagerten IT-Verbund die Gefährdungslage bewertet werden (IT-Security Dashboard). Dies ermöglicht weiter eine zügige, automatische Anpassung der Liste mit den vor Ort umzusetzenden Sicherheitsmaßnahmen.

Insgesamt wird also die Umsetzung eines Informationssicherheitsmanagements für die Behörden deutlich erleichtert und das Sicherheitsniveau erhöht. Zusätzlich erfahren Behörden Unterstützung bei der Sicherheitsevaluierung nach IT-Grundschutz.

7 Fazit und Ausblick

In dieser Arbeit wurde ein neues Konzept präsentiert, das es dem IT-Personal in Bürgerämtern ermöglicht, ihre kritischen IT-Infrastrukturen hinsichtlich der Mindestanforderungen zu beurteilen und abzusichern. Durch den gewählten Ansatz der Auslagerung komplizierter Sicherheitsmaßnahmen und deren Beurteilung von externen Dritten (Zertifizierung) ist es auch für Behörden mit geringem technischen Know-How und Ressourcen möglich ein ISMS zu etablieren. Aufgrund ähnlicher Infrastrukturen können Behördenprofile erstellt und einzelne Komponenten ausgelagert werden. Sowohl zentrale als auch dezentrale Maßnahmen müssen für ein lückenloses IT-Sicherheitskonzept aufeinander abgestimmt und umgesetzt werden.

Im nächsten Schritt werden grafische Benutzeroberflächen als Mock-ups skizziert, die zunächst heuristischen Usabilitytests unterzogen [CMN08] und entsprechend verbessert werden. Im Rahmen des Projektes nutzen wir das gewonnene Feedback um die Prototypen zu verbessern. Anschließend werden diese Prototypen im Rahmen von empirischen Usabilitytests den Anwendern vorgelegt. Durch das Beobachten der Interaktionen mit den Prototypen und dem dadurch gewonnenem Feedback können überarbeitete Prototypen erstellt werden, die iterativ validiert werden sollen.

Bei der funktionalen Umsetzung ist darauf zu achten, dass aktuelle IT-Sicherheitsstandards eingehalten werden. Hierfür wird der BSI-Grundschutz als Vorgabe genutzt, der der Normenreihe ISO 2700x angelehnt ist.

Im weiteren Projektverlauf soll geprüft werden, ob die Ergebnisse auf andere Bereiche übertragen sind: Die evaluierten Konzepte könnten auf weitere Sektoren und Branchen kritischer Infrastrukturen anwendbar sein.

Weitere zu klärende Fragen betreffen insbesonders rechtliche Aspekte. So agiert in unserer Lösung der SecMaaS-Anbieter im Namen der Behörde, siehe z.B. Abschnitt 6.1. Weiter fallen z.B. bei der Umsetzung eines zentralen Intrusion Detection System (Abschnitt 6.2) behördenspezifische Daten an. Ob solch ein Dienst damit von einem privaten Anbieter übernommen werden kann, ist zunächst fraglich und muss untersucht werden. Alternativ bietet sich ein Unternehmen an, das sich im staatlichen Besitz befindet oder der Cloud-Dienst wird in einer Behörde umgesetzt. Der Bund betriebt bereits mehrere IT-Dienstleistungszentren, z.B. die Bundesstelle für Informationstechnik als Abteilung des Bundesverwaltungsamts im Geschäftsbereich des Bundesministeriums des Innern oder Zentrum für Informationsverarbeitung und Informationstechnik (ZIVIT) im Geschäftsbereich des Bundesfinanzministeriums.

Literatur

[Ape04] Apelbaum, Y. *User Authentication Principles, Theory and Practice*. Technology Press, 2004.

[Bun15] Bundesamt für Sicherheit in der Informationstechnik: Lagebericht IT-Sicherheit 2015, 2015.

[Bun16] Bundesamt für Sicherheit in der Informationstechnik: Anforderungskatalog Cloud Computing – Kritierien zur Beurteilung der Informationssicherheit von Cloud-Diensten, 2016.

[CMN08] S.K. Card, T.P. Moran, and A. Newell. *The Psychology of Human-Computer Interaction*. CRC Press, repr edition, 2008.

[dI11] Bundesministerium des Innern. Sektoren- und Brancheneinteilung Kritischer Infrastrukturen, 2011.

[DRS10] F. Doelitzscher, C. Reich, and A. Sulistio. Designing Cloud Services Adhering to Government Privacy Laws. In *Computer and Information Technology (CIT)*, 2010.

[FHMS12] S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a Service – Usable Security for the Cloud. In *Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2012.

[KC12] D. Krishnan and M. Chatterjee. Cloud security management suite – Security As a Service. In *Information and Communication Technologies (WICT)*, 2012.

[MKL09] T. Mather, S. Kumaraswamy, and S. Latif. *Cloud Security and Privacy – An Enterprise Perspective on Risks and Compliance*. O'Reilly Media, 2009.

[MLM15] S.C. Mallam, M. Lundh, and S.N. MacKinnon. Integrating human factors & ergonomics in large-scale engineering projects: Investigating a practical approach for ship design. *International Journal of Industrial Ergonomics*, 50, 2015.

[PMW11] H. Plattner, C. Meinel, and U. Weinberg. *Design Thinking: Innovation lernen – Ideenwelten öffnen*. mi-Wirtschaftsbuch, 2011.

[PT11] M. Peter and G. Timothy. The NIST Definition of Cloud Computing, 2011.

[Rus16] F. Rustler. *Denkwerkzeuge der Kreativität und Innovation: das kleine Handbuch der Innovationsmethoden*. Midas Management Verlag AG, 3. Auflage, 2016.

[ZMR10] Y. Zhang, F. Monrose, and M. K. Reiter. The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis. page 176. ACM Press, 2010.