Schatten-IT – Ein unterschätztes Risiko?

Christopher Rentrop · Stephan Zimmermann · Melanie Huber

HTWG Konstanz – kips
{rentrop | stephan.zimmermann | melanie.huber}@htwg-konstanz.de

Zusammenfassung

Der Begriff Schatten-IT beschreibt Systeme, die außerhalb des Verantwortungsbereiches der IT durch die Fachabteilung eigenständig entwickelt und betrieben werden. Obwohl dieses Phänomen weit verbreitet ist, blieb diese Schatten-IT in Wissenschaft und in Praxis lange unbeachtet. Seit einiger Zeit ist eine verstärkte Auseinandersetzung mit dem Phänomen erkennbar. Jedoch gibt es bisher nur wenige empirisch gestützte Erkenntnisse über die Schatten-IT. Diese Lücke wird in dem vorliegenden Beitrag angegangen. Auf Basis von vier Fallstudien werden die Verbreitung, Verwendung und die Qualität der Schatten-IT ermittelt. Dabei zeigt sich, dass die Schatten-IT mit durchaus erheblichen Risiken verbunden sein kann. Demgegenüber bleibt die Qualität jedoch merklich zurück. Erkennbar ist dabei auch, dass die Schatten-IT nicht im Blickfeld der Kontrollsysteme der Unternehmen erscheint. Durch Maßnahmen wie die Steigerung der Awareness der Schatten-IT im Unternehmen sowie eine Entwicklung der Schatten-IT hin zu einer gesteuerten Fachbereichs-IT lassen sich die Risiken wirksam reduzieren. Zudem sind die Kontrollsysteme der Unternehmen so anzupassen, dass auch die Schatten-IT in diesen sichtbar wird.

1 Einleitung

In vielen Unternehmen betreiben und entwickeln die Fachabteilungen eigene IT-Systeme außerhalb des Einflussbereiches der IT-Abteilung. [Chej12] Dieses Phänomen wird auch als Schatten-IT bezeichnet. Eine wesentliche Eigenschaft dieser Schatten-IT besteht darin, dass sie nicht in das IT-Servicemanagement des Unternehmens eingebunden ist. [ZiRe12]

Zwar ist diese Schatten-IT sehr weit verbreitet, jedoch findet das Thema in vielen Unternehmen nur eine geringe Aufmerksamkeit. Eine Ursache dafür scheint zu sein, dass die potenziellen Auswirkungen der Schatten-IT als gering eingeschätzt werden. Die Unternehmen verlassen sich in dem Zusammenhang auf die Funktionsfähigkeit ihrer Kontrollsysteme und erwarten, dass der Rest „unkontrollierter“ Datenverarbeitung nur einen geringen Einfluss auf das Unternehmen hat.

Ziel des vorliegenden Beitrages ist es, diese Annahme kritisch zu hinterfragen und zu untersuchen, welches Risiko tatsächlich in der Schatten-IT steckt. Damit wird auch geprüft, ob die bestehenden Kontrollsysteme hinreichend konzipiert sind und zielgerichtet angewendet werden. Darüber hinaus soll analysiert werden, welche Maßnahmen zu einer vermehrten Auseinandersetzung mit der Schatten-IT führen können. Durchgeführt wird diese Untersuchung auf Basis von vier Fallstudien, bei denen die Schatten-IT in verschiedenen Fachbereichen in unterschiedlichen Unternehmen erhoben wurde.

P. Schartner · K. Lemke-Rust · M. Ullmann (Hrsg.) · D•A•CH Security 2015 · syssec (2015) 291-300.

Im nachfolgenden Kapitel wird zunächst der Begriff Schatten-IT und ihre Auswirkungen insbesondere auf die IT-Sicherheit erläutert. Anschließend werden die Vorgehensweise und die Ergebnisse der durchgeführten Fallstudien aufbereitet. Im letzten Abschnitt werden mögliche Maßnahmen beschrieben, die zu einer höheren Aufmerksamkeit für das Thema Schatten-IT in Bezug auf Kontrollsysteme beitragen können.

2 Fachliches Umfeld

Zur Einführung in das Themengebiet werden nun zunächst der Begriff „Schatten-IT“ und die Managementansätze aus der Literatur beschrieben.

2.1 Definition

Schatten-IT ist geschäftsprozessunterstützend, aber nicht in das IT-Servicemanagement eingebunden. [ZiRe12] Ein typisches Beispiel hierfür ist die individuelle Datenverarbeitung (IDV) mit Tabellenkalkulationen und kleineren Datenbankanwendungen. [HaLK08] Genauso zählt aber auch die Nutzung von Cloud-Services und selbst beschafften mobilen Endgeräten für geschäftsprozessunterstützende Aufgaben dazu. Schließlich betreiben die Anwender komplexe Systemlandschaften, bei denen sie von der Hardware- und Softwarebeschaffung bis zur Anwendungsunterstützung die gesamte IT-Wertschöpfungskette abdecken. Hierunter fällt in vielen Unternehmen auch die „Shop-Floor-IT“ in den Produktionsmaschinen.

Ein wesentlicher Treiber für die Schatten-IT ist ein mangelhaftes Alignment von Fachbereich und IT. [GCUB12] Die vergrößerte organisatorische Distanz zwischen den beiden Organisationseinheiten erhöht die Wahrscheinlichkeit der Entstehung von Schatten-IT. Jedoch zeigen die Erfahrungen in der Praxis, dass auch bei einem guten Alignment Schatten-IT entstehen kann, wenn der Fachbereich eine eigene Implementierung als schneller empfindet.

Aus der Schatten-IT ergeben sich per Definition zahlreiche Risiken; [Behr09] insbesondere für Datensicherheit und Datenschutz [PaPo13] [SiBa14] und Compliance. [SiDo12] Schatten-IT hat einen häufig ungeplanten Charakter und wird mit geringerer Professionalität im Vergleich zu offizieller IT entwickelt. In vielen Fällen unterbleibt die Analyse schutzbedürftiger Daten, so dass unternehmensweite Datenschutzkonzepte ungenügend sein können. Darüber hinaus werden häufig weder ausreichende Tests durchgeführt noch entsprechende Dokumentationen erstellt. Dies führt dazu, dass Fehler in den Anwendungen auftreten können. Schließlich ist Schatten-IT im Ursprung nutzerzentriert. Dies kann dazu führen, dass intransparente Lösungen, Ausfallrisiken und Abhängigkeiten von Einzelpersonen entstehen.

2.2 Management

In der Literatur werden verschiedene Maßnahmen zum Management der Schatten-IT vorgeschlagen. [ZiRF14] [FüRo14] Grundlage des Managements ist eine risikoorientierte Vorgehensweise, welche ausgehend von den potenziellen Schäden, eine entsprechende Steuerung der Schatten-IT ableitet.

Als Teilaufgaben werden im Einzelnen die Erhebung, Bewertung und Steuerung der Schatten-IT gesehen. Im Rahmen der Erhebung sollen die vorhandenen Schatten-IT Systeme aufgedeckt werden. Umgesetzt werden kann dies mit einer Beschreibung der Geschäftsarchitekturen. Auf Basis der Erhebung ist dann eine entsprechende Bewertung der Systeme vorzunehmen. Zentrale Bewertungskriterien sind dabei die Qualität und die Relevanz der Schatten-IT Instanzen. Die

Bewertung wiederum bildet den Ausgangpunkt für Handlungsempfehlungen im Umgang mit einzelnen Systemen. Dabei soll vor allem durch die Koordination von Teilaufgaben zwischen Fach- und IT-Bereich die Qualität der vorhandenen Systeme verbessert werden. Eine Neuentwicklung ist vorzunehmen, wenn die Systeme aus technischen Gründen nicht grundlegend verbessert werden können. Falls die Qualität für das gegebene Einsatzgebiet ausreicht, genügt es, die Systeme im IT-Servicemanagement zu registrieren.

3 Vorgehensweise

In vier Fallstudien wurden Unternehmen verschiedener Branchen betrachtet. In Tabelle 1 sind die wesentlichen Kerndaten der Unternehmen wiedergegeben:

Tab. 1: Untersuchte Unternehmen

Name	A	B	C	D
Branche	Versicherung	Maschinenbau	Elektronik	Bank
Land	Schweiz	Deutschland	Deutschland	Deutschland
Mitarbeiter	1.300	11.500	5.500	500
Betrachtete Abteilungen / Prozesse	Leistungs-abwicklung	Auftrags-abwicklung	Marketing	Operations, Asset Management & Risikomanagement

In der Untersuchung wurden Interviews mit den relevanten Ansprechpartnern der entsprechenden Fachbereiche geführt. Die Interviews richteten sich nach der Leitfrage „Welche Tätigkeiten werden mit welchen IT-Systemen unterstützt?“. Auf Basis der vorhandenen Dokumentation des IT Managements wurde anschließend identifiziert, welche Systeme autonom im Fachbereich betrieben wurden und daher als Schatten-IT zu gelten hatten. Diese Systeme wurden dann hinsichtlich ihrer Qualität und Relevanz bewertet.

4 Ergebnisse

Nachfolgend werden die Ergebnisse der vier Fallstudien hinsichtlich des Aufkommens, der Qualität und der Relevanz der Schatten-IT in den Unternehmen aufbereitet. Auf Basis der Bewertung werden die entsprechenden Handlungsempfehlungen abgeleitet. Anschließend erfolgt außerdem eine Analyse der Funktionsfähigkeit der Kontrollsysteme in den Unternehmen.

4.1 Aufkommen

Schatten-IT Systeme konnten in allen untersuchten Bereichen entdeckt werden. Die Spanne ging dabei von 6 Systemen (Fallstudie A) bis zu 52 Systemen (Fallstudie B) pro Bereich. Insgesamt wurden in den Fallstudien 386 Schatten-IT Anwendungen erhoben. Eine einzelne Anwendung wurde dabei anhand der unterstützten Tätigkeiten abgegrenzt. Im Ergebnis kam es daher vor, dass eine Anwendung beispielsweise aus mehr als einer Excel-Datei bestand.

Bei der Erhebung der Systeme wurde auch betrachtet, auf welcher technischen Grundlage die Lösungen basieren. Eine wesentliche Gruppe bildete der oft als Individuelle Datenverarbeitung (IDV) bezeichnete Einsatz von durch die IT bereitgestellten Standard-Büroanwendungen. Daneben beschafften die Anwender aber auch eigene Software, die entweder wie beispielsweise Matlab lokal installiert wurde oder wie beispielsweise SalesForce.com direkt als Cloud Service genutzt werden konnte. Schließlich haben die Fachbereiche auch selbst komplexe Lösungen

entwickelt, bei denen die Anwender die gesamten Beschaffungs- und Betriebsprozesse für Hard- und Software durchgeführt haben.

Hinsichtlich der Umsetzung fällt auf, dass in der Bank und Versicherung die IDV die technische Basis für den überwiegenden Anteil der Systeme bildete. In den beiden Industrieunternehmen war die technische Grundlage wesentlich breiter gestreut. Dies scheint jedoch aufgrund der Aufgaben in den betrachteten Abteilungen naheliegend zu sein. In Tabelle 2 sind die jeweiligen Anteile der Lösungsansätze in den Fallstudien aufgelistet.

Tab. 2: Anteile verschiedener Schatten-IT Lösungen

	Bank und Versicherung (A,D)	Industrie (B,C)
Kombinierte Lösungen (Server und Software)	0%	37%
Cloud Services	0%	10%
Anwenderprogramme	13%	31%
IDV (z.B. Excel, Access, Outlook)	87%	20%

4.2 Qualität

In den Projekten wurde die Qualität der Schatten-IT auf einer Skala von 1-10 bewertet. Als Maßstab für die Qualität wurde beispielsweise die Integration der Systeme in die Prozesse betrachtet. Darüber hinaus wurde auch die Abdeckung aller für die Bereitstellung der Systeme notwendigen Teilaufgaben wie etwa Dokumentation oder Testen untersucht.

In Abbildung 1 sind die Qualitätsniveaus der gefundenen Schatten-IT Lösungen dargestellt; hierbei ist jeweils der Anteil der Lösungen den entsprechenden Qualitätsniveaus zugeordnet. Beispielsweise wurden ca. 20% aller Anwendungen in Bank und Versicherung in der Stufe „6“ eingeordnet.

Aufgrund der mangelnden Dokumentation und auch der fehlenden Revisionssicherheit einiger Anwendungen wurden die Schatten-IT Systeme in Bank und Versicherung im Schnitt etwas schlechter bewertet.

Die Analyse der Qualität der gefundenen Schatten-IT Lösungen zeigt auf der einen Seite eine teilweise überraschend hohe Qualität der technischen Umsetzung der Systeme. In einigen Fällen wurden durch die Fachabteilungen „professionelle“ Programmierframeworks angewendet.

Jedoch ist darüber hinaus zu erkennen, dass wie oben beschrieben die Qualität der Systeme durch die ungeplante Vorgehensweise gelitten hat. Es waren kaum entsprechende Dokumentationen der Systeme vorhanden, was eine erhebliche Abhängigkeit von den Entwicklern der Systeme mit sich brachte. Zudem erfolgte die Technologiewahl naturgemäß auf Basis der Vorlieben und Kompetenzen der Entwickler. Eine sachorientierte Entscheidung in dieser Frage unterblieb in der Regel. Dies führte in verschiedenen Fällen zu technisch nachteiligen Lösungen.

Ebenfalls spielte die IT-Sicherheit wie erwartet bei den Überlegungen der Fachbereiche nur eine untergeordnete Rolle. Dies führte zu teilweise erheblichen Sicherheitsrisiken im Hinblick auf die Vertraulichkeit unternehmensinterner Informationen, die Integrität von Entscheidungen sowie die Compliance.

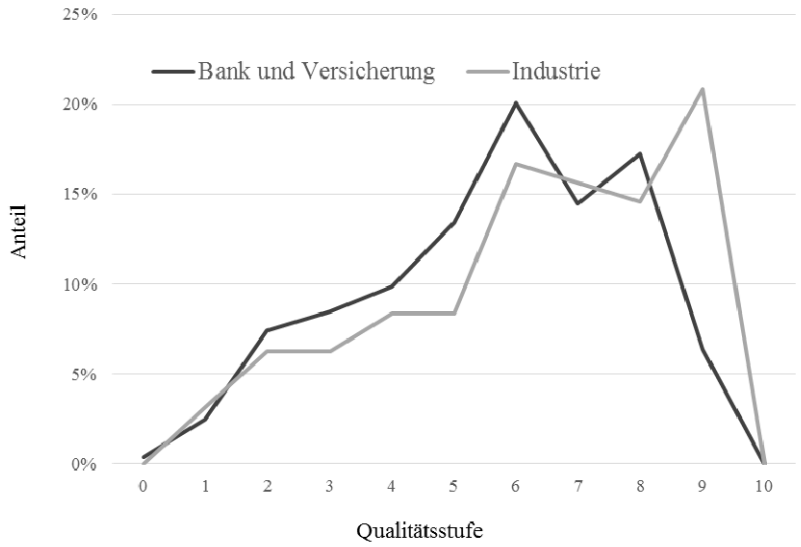

Abb. 1: Qualitätsniveau der Schatten-IT in den Branchen

Schließlich lässt sich den Daten auch entnehmen, dass die IDV in den Unternehmen teilweise bei Aufgaben Verwendung findet, für die sie nicht geeignet ist. Dies lässt sich daraus ableiten, dass die IDV Lösungen im Schnitt schlechter bewertet werden als Anwendungen mit einer anderen technischen Grundlage. Offensichtlich wird die IDV in Anwendungsszenarien eingesetzt, für die sie grundsätzlich nicht gedacht ist. Die falsche Verwendung der Technik lässt sich zum einen auf die leichte Verfügbarkeit dieser Werkzeuge zurückführen. Zum anderen scheinen solche Lösungen auf den ersten Blick leicht zu entwickeln zu sein, jedoch überschätzen die Anwender manchmal ihre Kenntnisse.

In Abbildung 2 sind die Qualitätsniveaus der verschiedenen Plattformen dargestellt:

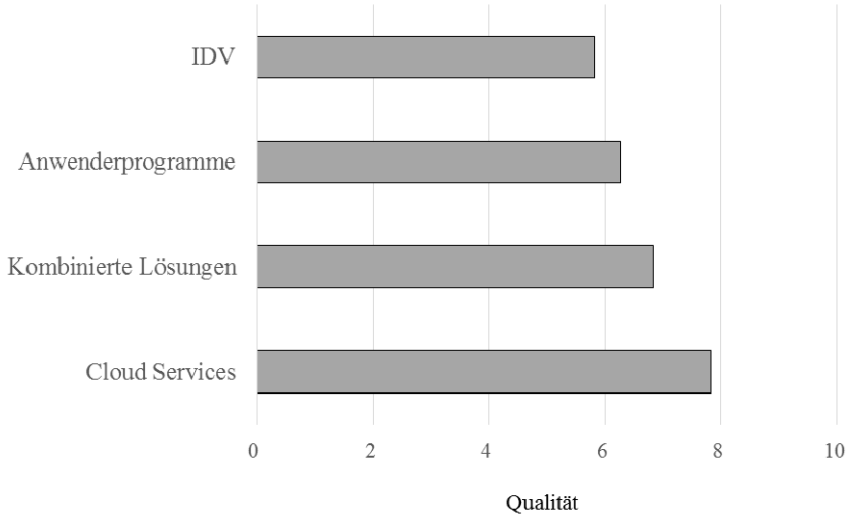

Abb. 2: Qualitätsniveau der Schatten-IT Lösungen

4.3 Relevanz

Neben der Qualität wurde auch die Relevanz der Schatten-IT für die Prozesse der Unternehmen analysiert. Die Relevanz wurde beispielsweise danach bewertet, ob mit den Systemen Entscheidungen getroffen werden, rechnungslegungsrelevante Sachverhalte aufbereitet werden oder eine andere Außenwirkung mit den Systemen verbunden ist. Bei der Betrachtung spielte die Kritikalität des Prozesses im Sinne einer Business Impact Analyse ebenfalls eine Rolle. In Abbildung 3 sind die Anteile der Schatten-Systeme bezogen auf die Kritikalität der unterstützten Prozesse sowie ihr Einfluss auf das Prozessergebnis dargestellt.

Die Erwartung vieler IT-Verantwortlicher, dass Schatten-IT nur eine geringe Relevanz hat und daher vernachlässigt werden kann, ist eindeutig zu widerlegen. Etwa 55% der gefundenen Schatten-IT Systeme waren prozessrelevant, das heißt die Durchführung des Prozesses war von der Funktionsfähigkeit der Schatten-IT abhängig. Der restliche Teil der Schatten-IT war prozessbegleitend, d.h. hier wurden Auswertungen über die Prozesse sowie Validierungen erstellt.

Etwas mehr als 1/3 der Schatten-IT betraf Prozesse, die für die Geschäftsmodelle der Unternehmen kritisch waren; als besonders kritisch wurden Prozesse mit einer erlaubten Ausfallzeit von maximal einem Tag angesehen. Im Ergebnis bedeutet dies, dass etwa 16% der gefundenen Systeme (also insgesamt 64 Schatten-Systeme in den 4 Unternehmen) durchführungsrelevant für hochkritische Prozesse waren. Vor dem Hintergrund vielfach mangelhafter Dokumentation ergaben sich hieraus erhebliche Risiken für das Business Continuity Management. Diese Risiken sind auch deswegen bemerkenswert, da keines der Systeme im Rahmen des Risikomanagements entdeckt wurde. Und das obwohl es in allen betrachteten Unternehmen ein entsprechendes Risikomanagementsystem gab. Dies ist darauf zurückzuführen, dass aufgrund der oben beschriebenen Erwartung seitens der Fachbereiche (und auch der IT), die möglichen Gefahren der Schatten-IT systematisch unterschätzt werden.

		Ist der Prozess von der Schatten-IT abhängig		
		Nein	Ja	
Wiederanlaufzeit des Prozesses gem BIA	1 Tag	20,15%	16,33%	36,48%
	1-3 Tage	9,95%	17,86%	27,81%
	3+ Tage	15,31%	20,41%	35,71%
		45,41%	54,59%	100,00%

Abb. 3: Bedeutung der Schatten-IT für die Prozesse

Im Hinblick auf die Verwendung der Schatten-IT ist festzuhalten, dass etwa 40% der gefundenen Schatten-IT entscheidungsrelevant war. Dies bedeutet, dass betriebliche Entscheidungen über Kredite, Lieferzusagen etc. auf Basis von Schatten-IT Systemen getroffen wurden. Hier machte sich insbesondere bemerkbar, dass es in vielen Fällen keine Änderungskontrolle über die Schatten-Systeme gab. Im Nachhinein war die Begründung für Entscheidungen kaum noch verifizierbar.

4.4 Handlungsempfehlungen

Auf Basis der Beurteilung der Qualität und der Relevanz lassen sich die oben skizzierten typischen Handlungsalternativen im Umgang mit den gefunden Schatten-IT Instanzen ableiten.

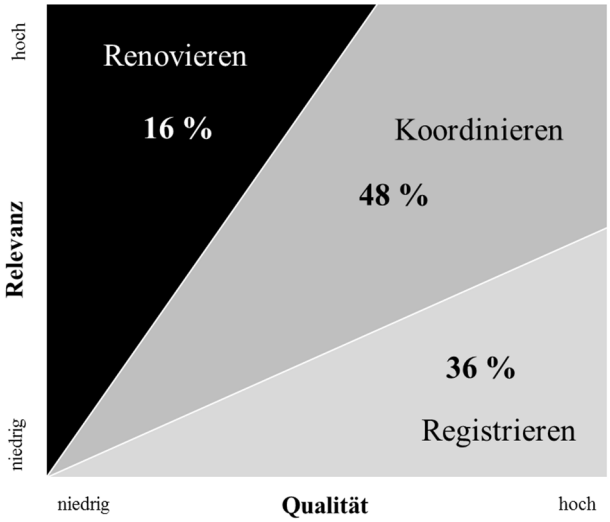

Abb. 4: Anteile der Basisstrategien im Umgang mit der Schatten-IT

In Abbildung 4 sind diese dargestellt und werden nachfolgend erläutert:

- Beim Registrieren wird die Existenz der Schatten-IT Anwendung zur Kenntnis genommen. Weitere unmittelbare Schritte erfolgen nicht, da die Qualität der Systeme in Relation zur Relevanz sehr hoch ist. Allerdings führt die Aufnahme der Instanz in das Architekturmanagement zu einer verbesserten Planung der Infrastruktur und entsprechender Projekte. In den Fallstudien betraf das etwa 36% der Systeme. Vor dem Hintergrund des Anteils der IDV von über 50% wird damit auch deutlich, dass bei einer Betrachtung der Schatten-IT auch die IDV und damit insbesondere die Tabellenkalkulationen einbezogen werden müssen.
- Im Bereich „Koordinieren“ werden Systeme mit einem immer noch ausgewogenen Verhältnis von Relevanz und Qualität durch eine verbesserte Arbeitsteilung von Fachbereich und IT qualitativ spürbar verbessert. In den Projekten betraf dies etwa 48% der Systeme. Bei vielen Systemen in dieser Gruppe waren die notwendigen Maßnahmen relativ einfach umzusetzen; beispielsweise durch die Einführung einer durch die IT unterstützen Versionierung der Systeme. In diesen Fällen wurde somit das oben beschriebene Problem der Änderungskontrolle gelöst.
- Systeme, die aufgrund ihrer Struktur für die unterstützte Aufgabe ungeeignet sind, sollten durch eine Neuentwicklung abgelöst werden („Renovieren“). Dies waren ca. 16% aller Systeme. In der Regel war eine falsche Technikwahl die Ursache. In Fallstudie B zum Beispiel musste eine MySQL Datenbank aufgrund der zu erwartenden Datenmenge abgelöst werden.

4.5 Funktionsfähigkeit der internen Kontrollsysteme

Wie in der Einleitung beschrieben, erwarten die Unternehmen, dass ihre internen Kontrollsysteme funktionieren. Ein Beispiel für ein solches Kontrollsystem ist das Verbot von IT-bezogenen Beschaffungen an der IT vorbei, das mit Hilfe des Einkaufes umgesetzt werden

solle. Daneben zählte auch der Entzug von Administratorrechten zu den gängigen Schutzmechanismen.

Diese Kontrollsysteme wirken jedoch nur eingeschränkt; beispielsweise ist es den Einkaufsabteilungen kaum möglich jeden Lieferanten zu überwachen und aus den Lieferantenrechnungen ist ein IT-Bezug nicht immer erkennbar.

Darüber hinaus können solche Kontrollmechanismen sogar kontraproduktiv wirken. Wird über ein stark reglementiertes Sourcing den Benutzern der Weg an den Beschaffungsmarkt versperrt, erstellen Sie gewünschte Lösungen mit den vorhandenen Mitteln selbst. Bei den Auswertungen wird jedoch erkennbar, dass die eigenerstellten Lösungen in der Regel weniger für die Aufgaben geeignet sind, als Lösungen, die mit externer Unterstützung erstellt wurden. Zudem führt eine solche rigide Kontrolle zu einer vermehrten Verwendung von IDV Lösungen, was wie oben erläutert ebenfalls einen negativen Effekt auf die Qualität hat. In Abbildung 5 wird der Zusammenhang zwischen Sourcing und den getroffenen Maßnahmen verdeutlicht.

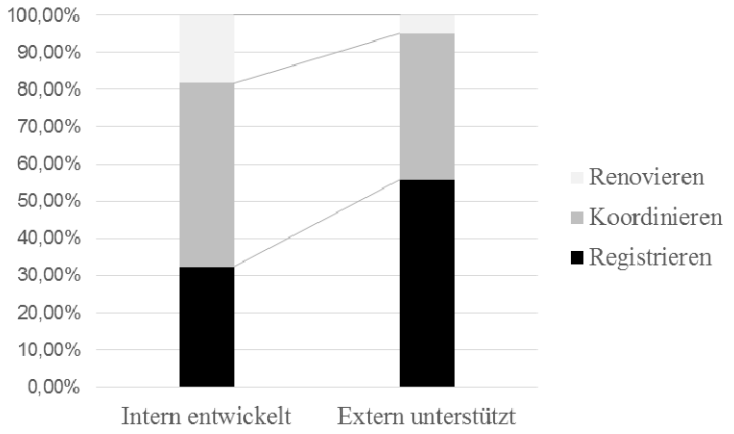

Abb. 5: Der Einfluss des Sourcing auf die Schatten-IT Instanzen

Wie oben dargestellt zeigt sich auch, dass bis auf wenige einzelne Ausnahmen, diese Systeme nicht im Risikomanagement der Unternehmen berücksichtigt und damit die damit verbundenen Risiken nicht als solche erkannt wurden. Zudem ist hervorzuheben, dass diese Schatten-IT Instanzen auch bei internen und externen Prüfungen unentdeckt blieben. Daraus lässt sich ableiten, dass die Schatten-IT eine Schwäche im Management der Informationssicherheit darstellt und somit die ISMS überprüft werden sollten.

5 Maßnahmen

Die Ergebnisse aus den Studien in den vier Unternehmen belegen, dass die Funktionsfähigkeit der Sicherungsmechanismen erheblich überschätzt wird. Nachfolgend soll daher skizziert werden, wie die Unternehmen diese Lücke schließen können. Dies kann dabei einerseits durch die Förderung der Awareness geschehen, wodurch die Schatten-IT in den bisherigen Kontrollsystemen mehr Beachtung finden soll. Andererseits kann auch ein eigenes Kontrollsystem für Schatten-IT eingeführt werden.

5.1 Förderung der Awareness

Das Versagen der Kontrollmechanismen ist unter anderem auf das Unterschätzen der Auswirkungen zurück zu führen; damit ist auch ein sich selbst verstärkender Effekt verbunden. Die

Fachbereiche erwarten keine Risiken in ihrer Schatten-IT. Sie wenden dementsprechend wenig für die Sicherheit der eigenen Systeme auf und nehmen diese daher aber auch nicht in ihr Risikomanagement auf. Im Ergebnis führt dies dazu, dass den Fachbereichen das Schadenspotenzial nicht bewusst ist. Nach Aufdeckung der Risiken im Rahmen der Erhebung waren die beschriebenen Probleme allseits unstrittig. Im Ergebnis hätte es also schon gereicht, die potenzielle Relevanz der Schatten-IT höher zu gewichten, um diese als wichtig genug zu erachten, sie in die bekannten und gelebten Kontrollprozesse mit aufzunehmen. Voraussetzung hierfür ist jedoch die „Awareness“ dieses Themas.

Dementsprechend bestünde ein Ansatz für Unternehmen die Mitarbeiter und Führungskräfte im Hinblick auf die potenziellen Gefahren der Schatten-IT und insbesondere auch der IDV zu schulen und sie damit anzuhalten, die üblichen Kontrollprozesse auch in diesem Thema einzuhalten. Ansätze für solche Schulungen bieten prominente Beispielfälle aus den jeweiligen Unternehmen. Des Weiteren könnte das Thema Schatten-IT auch in Standard-Schulungsprogramme zur IT-Sicherheit und insbesondere zu Security Awareness eingebunden werden. Ein weiterer Ansatzpunkt wäre auch der Einsatz von Lernspielen zum Thema Schatten-IT. Darüber hinaus sollte die Schatten-IT auch explizit in den Leitlinien zum Risikomanagement thematisiert werden.

5.2 Management der Schatten-IT

Neben der verbesserten Wahrnehmung der Schatten-IT in den bestehenden Kontrollstrukturen kann es auch sinnvoll sein, eigene Strukturen für eine in den Fachbereichen angesiedelte, dezentralisierte IT zu entwickeln.

Dies umfasst in erster Linie die (erstmalige) Durchführung eines Schatten-IT Projektes mit den oben skizzierten Maßnahmen der Erhebung, Bewertung und Steuerung der Schatten-IT. Ein solches Projekt kann dabei versuchsweise in einzelnen Bereichen mit besonderem Bedarf an Informationssicherheit begonnen werden. Diese Projekte ermöglichen einerseits, die Risiken im Unternehmen abzuschätzen. Andererseits bewirken sie als „Quick wins“ aber auch schon einer Veränderung in der Zusammenarbeit von Fachbereich und IT. Wichtig ist hierbei, dass im Rahmen solcher Projekte Schatten-IT nicht nur als etwas Bedrohliches wahrgenommen werden sollte, sondern auch der positive Wertbeitrag dieser dezentralen Lösungen anzuerkennen ist. Ein solcher Ansatz erhöht die Erfolgsaussichten, da in dem Fall die Schatten-IT durch die Fachbereiche nicht „versteckt“ werden muss.

Darüber hinaus ist aber auch eine Verstetigung des Managements der dezentralen IT anzustreben. Zu den Maßnahmen gehört beispielsweise die Entwicklung einer sachgerechten internen Richtlinie für die IDV beziehungsweise die dezentrale IT. Teilweise fehlen diese, teilweise gibt es auch IDV-Richtlinien, die zu umfangreiche Anforderungen stellen und daher weitgehend unbeachtet bleiben. Zudem sind die in vielen Unternehmen vorliegenden Richtlinien für IT-Governance und IT Sicherheit oftmals zu wenig aussagekräftig.

Es sind also Leitlinien zu entwickeln, welche Anwendungen und welche Teilaufgaben bei der Erbringung der IT-Services in der Verantwortung des Fachbereiches liegen und wie die IT diese dabei unterstützen und begleiten soll.

Schließlich wäre auch eine kontinuierliche Erhebung neuer Schatten-IT sinnvoll. Die Maßnahmen des Architekturmanagements in den Unternehmen sind entsprechend zu erweitern. Dabei ist jedoch auf einen geringen Erfassungsaufwand zu achten, da sonst die Fachbereiche in Versuchung geraten könnten, die Regeln wieder zu unterlaufen.

6 Zusammenfassung

In diesem Beitrag wurde gezeigt, dass die Schatten-IT in den Unternehmen oftmals eine wichtige Rolle in der Unterstützung der Geschäftsprozesse spielt. Gleichzeitig war in den Projekten auch zu erkennen, dass die Qualität der Schatten-IT ihrer Kritikalität oft genug nicht ausreichend gerecht wird. Damit wurde gleichzeitig auch deutlich, dass viele Unternehmensverantwortliche die Risiken der Schatten-IT systematisch unterschätzen und die vorhandenen Kontrollsysteme Lücken aufweisen.

In vielen Unternehmen liegen also Risiken im Verborgenen, welche erhebliche Auswirkungen auf die Informationssicherheit und Compliance haben können. Mit den skizzierten Maßnahmen können diese Risiken reduziert und auch das Vertrauen in die Kontrollsysteme wieder erhöht werden. Grundvoraussetzung hierfür ist jedoch die Schatten-IT als relevantes Problem im Unternehmen wahrgenommen wird und entsprechende Projekte initiiert werden.

Literatur

[Behr09] S. Behrens: Shadow systems: The good, the bad and the ugly. Communications of the ACM, 52 (2), (2009), S. 124–129.

[Chej12] T. Cheijfec: Shadow IT survey v3. (2012). http://chejfec.com/2012/11/03/shadow-it-infographic/shadow-it-survey-v3.

[FüRo14] D. Fürstenau, H. Rothe: Shadow IT systems: Discerning the good and the evil. 22nd European Conference on Information Systems. Tel Aviv, Israel (2014).

[GCUB12] A. Györy, A. Cleven, F. Uebernickel, W. Brenner: Exploring the Shadows: IT Governance approaches to User Driven Innovation. (Paper 222). Proceedings of the 20th European Conference on Information Systems (2012).

[HaLK08] G. Hagemeister, B. Lui, M. Kons: Individuelle Datenverarbeitung in den Unternehmen. Anforderungen aus Sicht der Ordnungsmäßigkeit. Zeitschrift Interne Revision (2), (2008), S. 76–80.

[PaPo13] R. R. Panko, D. N. Port: End User Computing. Journal of Organizational and End User Computing, 25 (3), (2013), S. 1–19.

[SiBa14] M. Silic, A. Back: Shadow IT – A view from behind the curtain. Computers & Security, 45, 2014) S. 274–283.

[SiDo12] A. Silvius, T. Dols: Factors influencing non-compliance behavior towards information security policies. International Conference on Information Resources Management. Vienne, Austria. (2012).

[ZiRe12] S. Zimmermann, C. Rentrop: Schatten-IT. HMD Praxis der Wirtschaftsinformatik, 49 (6), (2012), S. 60–68.

[ZiRF14] S. Zimmermann, C. Rentrop, C. Felden: Managing Shadow IT Instances – A Method to Control Autonomous IT Solutions in the Business Departments. (2014).