



Bewusster Einsatz von Schatten-IT: Sicherheit & Innovationsförderung

Walter Brenner
Andreas Györy
Mani Pirouz
Falk Uebernickel

Studien Nr.: SIT/ 01
Lehrstuhl: Prof. Dr. W. Brenner
Datum: 20.10.2011

**Universität St. Gallen -
Hochschule für Wirtschafts-, Rechts-
und Sozialwissenschaften (HSG)**

Institut für Wirtschaftsinformatik
Müller-Friedberg-Strasse 8
CH-9000 St. Gallen
Tel.: +41 / 71 / 224 3861
Fax: +41 / 71 / 224 3296

Prof. Dr. A. Back
Prof. Dr. W. Brenner (geschäftsführend)
Prof. Dr. H. Österle
Prof. Dr. R. Winter

Inhaltsverzeichnis

1	Management Summary	1
2	Was ist Schatten-IT?	1
3	Warum ist Schatten-IT heute ein relevantes Thema?	2
4	Technische Ausprägungen von Schatten-IT	4
5	Organisatorische Ausprägung von Schatten-IT	5
6	Prozesse, in denen Schatten-IT entsteht	6
7	Potentiale und Herausforderungen von Schatten-IT	7
8	Umgangsformen mit Schatten-IT	10
9	Zusammenfassung und Ausblick	10
10	Details zur Umfrage: „Umgang mit Schatten-IT“	11
11	Literaturverzeichnis	12

1 Management Summary

Durch aktuelle Trends wie „Mobile Computing“, „Cloud Computing“ und „Digital Natives“ wird das Thema der Steuerung von und Verantwortung für Informationssysteme neu entfacht. Mit dem zunehmenden Trend Richtung „Bring Your Own Device“ (BYOD) haben Mitarbeiter bereits die Verantwortung für das Sourcing und den Betrieb von mobilen Geräten im professionellen Einsatz übernommen und die Aufgabe der IT-Abteilung auf die Bereitstellung von Software, Services und der dahinterliegenden Infrastruktur eingeschränkt. Dies wird auch in dieser Studie bestätigt: Unternehmen machen im Umgang mit IT-Lösungen bei garantierter Datensicherheit einen Schritt zurück und lassen ihre Anwender entscheiden. Anders verhalten sich IT-Abteilungen bei Lösungen, die als Datensicherheitsrisiko eingestuft werden. Daher gelten für Software und Software as a Service (SaaS) Lösungen strenge Verhaltensregeln und technische Einschränkungen. Um die Strategien im Umgang mit unkontrollierten Lösungen vergleichbar und bewusst gestaltbar zu machen, wird in dieser Studie eine Klassifikation entwickelt, die Schatten-IT nach der technischen, prozessbezogenen und organisatorischen Ausprägung einstuft. Diese ermöglichen die gezielte Ausnutzung von Vorteilen und Minimierung von Risiken bei der Definition von Schatten-IT Strategien. So können durch Eigenverantwortung im Fachbereich während dem Konzeptions- und Sourcingprozess schnell interne und externe Lösungen ausprobiert, mit den Anwenderanforderungen abgeglichen und für kurzzeitige Lösungen oder isolierte Innovationsbereiche eingesetzt werden. Gleichzeitig kann durch Monitoring und Steuerung des Betriebs und der Nutzung geschäftskritischer IT-Systeme deren Datensicherheit und Verfügbarkeit garantiert werden.

Für diese Studie wurden daher zehn internationale Organisationen untersucht, um zu identifizieren, welche Formen von Schatten-IT auftreten und wie damit umgegangen wird.

2 Was ist Schatten-IT?

„Schatten-IT“ oder auch „Graue IT“ (engl. „Shadow IT“ oder „Rogue IT“) bezeichnet IT-Lösungen oder IT-Mitarbeiter¹, die in einem Unternehmen unabhängig von einer dedizierten IT-Abteilung zum Einsatz kommen. Diese werden von Fachbereichen genutzt und finanziert, wobei die IT-Abteilung darüber nicht informiert ist oder hierfür keine Verantwortung übernimmt (Zimmermann, Rentrop, & Laak, 2011). Durch Schatten-IT entstehen Risiken für das Unternehmen da Leistungen, die ursprünglich von der IT-Abteilung garantiert wurden (z.B. Datensicherheit, Verfügbarkeit und Kostentransparenz) bei Schatten-IT nicht mehr sichergestellt sind. Um dieses Risiko zu vermeiden, setzen IT-Verantwortliche meist strenge Richtlinien für Mitarbeiter sowie organisatorische und technische Kontrollmaßnahmen ein. Das kann jedoch den Geschäftsprozess bremsen und die anwendergetriebene Innovation vermeiden. Laut einer Studie von RSA (RSA Security Inc., 2007) haben 35% der Mitarbeiter in amerikanischen Unternehmen bereits die Notwendigkeit erlebt, Sicherheitsrichtlinien zu um-

¹ In dieser Studie werden Schatten-IT Mitarbeiter, die zusätzlichen Support für offizielle oder Schatten-IT Systeme bieten, nicht dediziert behandelt. Stattdessen wird auf die Studie von booz&co. zu Schatten Mitarbeiter verwiesen (Shining the Light on Shadow Staff, 2003).

gehen, um ihrer täglichen Arbeit nachgehen zu können. Wollen IT-Abteilungen den heute geforderten Spagat zwischen Innovation, Sicherheit und Kostensenkung meistern, ist es essenziell, Schatten-IT nicht - wie es heute häufig der Fall ist - als Tabu-Thema zu behandeln (Zeitler, 2011) und strenge(re) Restriktionen einzuführen, sondern gezielt den Verantwortungsbereich der IT-Abteilung neu zu gestalten. Es muss bewusst abgewogen werden, wann Transparenz und Kontrolle benötigt werden, um Risiken zu minimieren und Skaleneffekte zu erzielen und wo ein bewusstes Risiko in Kauf genommen werden sollte, um anwendergetriebene Innovation zu fördern.

3 Warum ist Schatten-IT heute ein relevantes Thema?

Mit der rasanten Entwicklung des Internets haben IT-Konsumprodukte Ende der neunziger Jahre den professionellen IT-Markt eingeholt und nehmen seitdem eine immer wichtigere Rolle in unserem täglichen privaten Leben ein (Meeker, Devitt, & Wu, 2010). Durch die gestiegene Anwenderorientierung dieser Produkte hat die heutige Generation gelernt selbständig, IT-Lösungen (bspw. Smartphones oder soziale Netzwerke) für private Zwecke zu konfigurieren und einzusetzen. Viele IT-Innovationen finden seitdem zuerst auf dem Konsummarkt statt, was laut Gartner zu einer Konsumorientierung (engl. Consumerization) in der Unternehmens-IT geführt hat (Escherich, 2011). IT-Lösungen, die ursprünglich für den Privatgebrauch entworfen wurden, wie bspw. Apples iPhone oder das iPad, finden so den Weg in die Unternehmen. Im Vergleich mit den Jahren vor der Jahrtausendwende ist heute der technologische Vorsprung in der Nutzung von IT-Systemen, von Unternehmen gegenüber ihren Mitarbeitern drastisch gesunken, vereinzelt sogar umgedreht (Gens, Levitas, & Segal, 2011). Diese technologische Ebenbürtigkeit ihrer Anwender stellt IT-Abteilungen vor neue Herausforderungen:

- Cloud Computing: Mitarbeiter können schnell alternative IT-Dienstleistungen und Software im Internet identifizieren und einsetzen
- Mobile Computing: Mitarbeiter erwarten mobilen Zugriff auf firmeninterne IT-Dienstleistungen in jeder Situation und an jedem Ort. Hierfür nutzen sie ihre eigene Infrastruktur
- Digital Natives: Mitarbeiter haben dieselben Ansprüche gegenüber IT-Lösungen im Unternehmen, wie sie das aus ihren privaten IT-Lösungen gewohnt sind.

Cloud Computing bezeichnet Dienste, die sowohl infrastruktur- (IaaS), entwicklungs- (PaaS) als auch geschäftsprozessorientierte (SaaS) Leistungen über das Internet bezogen werden. Da diese Dienstleistungen meist nach Nutzung und ohne Bereitstellungskosten verrechnet werden, ist dabei die finanzielle Hemmschwelle gering. Zusätzlich haben Anbieter die benötigte Infrastruktur bereits in Betrieb und die Bereitstellung automatisiert, so dass Dienstleistungen meist sofort nach der Bestellung verfügbar sind. Bewährte Dienste besitzen dabei eine stabile und intuitive Oberfläche, die auf beliebigen Endgeräten und ohne lokale Installation browserbasiert über das Internet ausführbar sind. Cloud Computing Dienste sind somit auch in Unternehmen verfügbar und stehen dadurch in Konkurrenz mit internen

Dienstleistungen. Dass dies eine akute Problemstellung für IT-Abteilungen ist, die nicht allein durch strengere Mitarbeiterrichtlinien gelöst werden kann, zeigt eine aktuelle Studie von Avandane (*Global Survey: Has Cloud Computing Matured?*, 2011). Diese besagt, dass im Durchschnitt ein Fünftel der befragten Führungskräfte bereits kostenpflichtige Cloud Dienste ohne das Wissen der IT-Abteilung bezogen haben. Grund für die Nutzung waren die Anwenderfreundlichkeit (61%) und Bereitstellungszeit (50%), wobei 27% der Befragten die IT-Abteilung darüber nicht informierte, da die Nutzung gegen Unternehmenssicherheitsrichtlinien verstoße.

Mobile Computing bezeichnet den heutigen Trend immer leistungsfähigere mobile Geräte zu nutzen, die über zunehmend höhere Bandbreiten mit dem Internet verbunden sind. Der rasante Zuwachs an funk-vernetzten Smartphones, Tablets, Netbooks, Notebooks und portablen Medien- und Spiele-Konsolen deckt inzwischen fast jede Altersklasse und Lebenssituation ab. Laut einer aktuellen Studie von Morgan Stanley (Meeker et al., 2009) werden bereits in drei Jahren weltweit mehr Anwender über mobile Endgeräte Web-Services beziehen als über Desktop Rechner. IT-Abteilungen verlieren durch mobile Datenverbindungen über Mobilfunkanbieter ihre frühere Rolle als einziger Internetprovider im Unternehmen und damit die Möglichkeit, die Nutzung von Internetdienste zu überwachen und steuern. Der Trend bedingt gleichzeitig, dass eine wachsende Anzahl an Mitarbeitern die mobile Verfügbarkeit der unternehmensinternen Services¹ erwartet. Wird dies ermöglicht, müssen die IT-Abteilungen sicherstellen, dass die Datensicherheit sowohl in der internen Infrastruktur als auch auf den mobilen Endgeräten gewährleistet wird. Dies wird zusätzlich dadurch erschwert, dass sich Anwender mit ihren mobilen Endgeräten identifizieren und diese deshalb selbst bestimmen und personalisieren möchten (Schüler, 2011). Schnell entsteht im Unternehmen eine breite Vielfalt an Geräten, auf denen die IT-Abteilung die Datensicherheit gewährleisten muss. Mit Mobile Computing ist damit eine neue anwendergetriebene Plattform entstanden, die nur noch teilweise von der IT-Abteilung kontrolliert und verantwortet werden kann.

Digital Natives (dt. „digitale Muttersprachler“) wird die Generation, die bereits in einer IT-durchdrungenen Umwelt aufgewachsen ist, genannt. Als Richtwert für Digital Natives wird das Geburtsjahr 1980 genannt (Holmes, 2008). Diese Generation hat IT-Geräte (z.B. Computer, Smartphones und Entertainmentsysteme) und Internetdienste (z.B. soziale Netze, Instant Messaging und kooperative Arbeitsumgebungen) bereits als ein selbstverständliches Gebrauchsgut (engl. „commodity“) kennengelernt. Damit geht auch die ununterbrochene private Erreichbarkeit und Vernetzung einher. Gleichzeitig versuchen auch Unternehmen, das Potenzial dieser Erreichbarkeit von Digital Natives zu nutzen. Dabei verschwimmen die Grenzen zwischen Privatleben und Arbeitsumfeld. Das bedeutet, dass Digital Natives auch im Büro nicht auf ihre gewohnte private IT-Umgebung verzichten und gleichzeitig auch zu Hause und unterwegs auf ihre Arbeitsumgebung zugreifen möchten. Sind gewohnte privat genutzte Services schneller, anwenderfreundlicher oder funktional den unternehmensinternen Services

¹ beispielsweise BI- und ERP- Systeme, Email, Kalender, Adressbuch oder Intranet-Zugriff

überlegen, nutzen Digital Natives diese auch für Geschäftsprozesse. Der professionelle Einsatz privater IT-Lösungen (wie z.B. das Weiterleiten von unternehmensinternen Emails auf ein privates Emailkonto oder die Nutzung von Upload-Sites) führt jedoch schnell zu einem Sicherheitsrisiko, da Unternehmensdaten auf eine intransparente und ungesicherte Infrastruktur übertragen werden.

Cloud Computing Dienste, Mobile Computing und Digital Natives sind aktuell Treiber von potentiellen Schatten-IT-Lösungen und werden dafür oft als besondere Risikofaktoren eingestuft, die kontrolliert oder vermieden werden müssen. Dabei können diese Trends auch Unternehmen Vorteile bieten. Cloud Computing Dienste können integriert werden (sofern die Datensicherheit garantiert werden kann) oder einen Indikator liefern, welche Anforderungen von der internen IT-Abteilung nicht ausreichend erfüllt werden. Mobile Computing kann die Mitarbeiterproduktivität und -verfügbarkeit erhöhen. Digital Natives können durch ihre gleichzeitige IT-Affinität und Kenntnis ihrer Geschäftsprozesse schnell neue IT-Lösungen und Verbesserungspotentiale an bestehenden IT-Lösungen identifizieren. Um zu untersuchen, wieweit Unternehmen das Potential von Schatten-IT nutzen und wie sie damit umgehen, wurden IT-Verantwortliche von zehn führenden Schweizer und Deutschen Organisationen zum Thema Schatten-IT befragt.

4 Technische Ausprägungen von Schatten-IT

Um zu verstehen was IT-Verantwortliche heute als Schatten-IT bezeichnen und in wie weit dies eine aktuelle Herausforderung für sie darstellt, haben wir diese Gruppe nach den technischen Formen Schatten-IT befragt. Die Ergebnisse zeigt Tabelle 1.

<i>Technische Ausprägungen</i>	<i>Praxisbeispiel</i>	<i>Gilt als Schatten-IT bei folgenden Unternehmen</i>	<i>Aktuelle Problemstellung bei folgenden Unternehmen</i>
Datenverbindung <i>privat im professionellem Einsatz</i>	Mobiler Abruf von Firmen-Emails über das private Heimnetzwerk.	A, C, E, H (4/10)	A, C, H (3/10)
Skripte <i>für intern unterstützte Software</i>	Excel Macros, Batch-Files, VBA Skripte	A, B ¹ , B ² , C, G, H (5/10)	A, B ¹ , C, D, E, F, G, H (8/10)
Hardware <i>für den mobilen Einsatz</i>	Smartphones, Tablets, Netbooks	A, B ¹ , B ² , C, E, F, G, I (7/10)	A, B ¹ , B ² , C, D, E, F, G, I, J (9/10)
Server (inkl. PaaS & IaaS) <i>im Eigenbetrieb & Drittanbieter</i>	Access Datenbank, Entwicklungsumgebungen (z.B. Application-Server)	A, B ¹ , C, D, E, F, G, H, I, J (10/10)	B ¹ , E, F (3/10)
Software as a Service <i>von Drittanbietern</i>	Rapidshare, Google Mail, Facebook	A, B ¹ , C, D, E, F, G, H, I, J (10/10)	A, B ¹ , C, D, E, G, H, I, J (9/10)
Software <i>Eigen- oder Fremdentwickelt</i>	Installierte Software (z.B. Skype), Selbstentwickelte BI Lösung im Fachbereich	A, B ¹ , B ² , C, D, E, F, G, H, I, J (10/10)	A, B ¹ , B ² , C, E, G, H, I (7/10)

Tabelle 1: Technische Ausprägungen von Schatten-IT³

¹ Genannt im Interview mit dem CEO des Unternehmen B

² Genannt im Interview mit dem CIO des Unternehmen B

³ Sortiert und schattiert nach der Häufigkeit der Nennung einer technischen Ausprägung als Schatten-IT

Von den befragten Unternehmen wurden alle Umfänge als Schatten-IT bezeichnet, bei denen fremde Software zum Einsatz kommt. Unternehmen sehen die größte Gefahr in Software as a Service (SaaS) Angeboten und eigen- und fremdentwickelter Software. Hier spielt in erster Linie die Datensicherheit eine große Rolle. Der Einsatz von Servern oder Serverdienstleistungen (PaaS, IaaS) gilt nur in wenigen Unternehmen mit technisch versierten Mitarbeitern als kritisch. Vereinzelt bereits nicht mehr zu Schatten-IT gezählt werden anwendergetriebene mobile Hardware-Devices. Trotzdem zählt heute das Thema der anwenderindividuellen Geräte fast bei allen Unternehmen zu den Herausforderungen der IT-Abteilung. Der Einsatz anwendergetriebener Skripte, die den Funktionsumfang der Standardsoftware erweitern, wird in den meisten Unternehmen unterstützt und gilt deshalb nur bei der Hälfte der Unternehmen als Schattenlösung. Skripte, die dabei einen geschäftskritischen Charakter annehmen, gelten dafür bei sieben Unternehmen als Problemstellung. Nicht als Schatten-IT wird die Nutzung privater Datenverbindungen für den professionellen Einsatz gewertet. Weniger als die Hälfte der Befragten sprachen hier von Schatten-IT und nur drei sahen darin eine Problemstellung. Hier spielt die inzwischen weit fortgeschrittene Verschlüsselung des Datenstroms auf Softwareebene eine entscheidende Rolle. Zusätzlich zu diesen häufig erwähnten Formen von Schatten-IT nannten die befragten Organisation die Freigabe interner Services (Unternehmen A) und interner Daten (Unternehmen E) über das Internet wie auch den IT-Support (Unternehmen G), der von einem Fachbereich erbracht wird, wenn die IT-Abteilung diesen nicht erfüllen kann.

Deutlich wird, dass das Thema der Datensicherheit bei Softwarelösungen noch nicht ausreichend gelöst werden konnte und daher hier unkontrollierte Lösungen als Schatten-IT gelten, da sie ein nicht abschätzbares Risiko darstellen. Gegenbeispiel sind hierfür Hardware-Devices und Datenverbindungen, bei denen durch Verschlüsselung auf Softwareebene bereits Datensicherheitslösungen zur Verfügung stehen. Hier zählen unkontrollierte Lösungen oft nicht mehr zur Schatten-IT. In Umgebungen, in denen die Datensicherheit gewährleistet ist, werden anwendergetriebene Eigenentwicklungen (z.B. Skripte) als positive Schatten-IT betrachtet. Hier gilt die Herausforderung, Funktionsverfügbarkeit und Support für Skripte, die einen geschäftskritischen Charakter annehmen, rechtzeitig abzusichern. Schatten-IT ist daher nicht prinzipiell eine Gefahr, sofern Datensicherheit und Verfügbarkeit garantiert werden können.

5 Organisatorische Ausprägung von Schatten-IT

Schatten-IT ist eine Form des Transparenz- und Kontrollverlusts der IT-Abteilung über IT-Systeme. Um zu identifizieren, welche Form von Kontroll- oder Transparenzverlust Schatten-IT ausmacht, haben wir IT-Verantwortliche nach den Formen von Schatten-IT befragt, die sie in ihrem Unternehmen erleben. Das Ergebnis ist in Tabelle 2 visualisiert.

Die Mehrheit der Befragten bezeichnen IT-Lösungen, die unerkannt bleiben, als Schatten-IT (*Ohne Monitoring*). Obwohl es technisch möglich wäre, diese transparent zu machen, würde dies eine kostenintensive, rechtlich problematisch und oftmals nicht notwendige Überwachung bedeuten. Sobald solche IT-Lösungen als geschäftskritisch identifiziert werden, kann

gezielt eine Überwachung oder eine Integration umgesetzt werden, um deren Verfügbarkeit sicherzustellen. Wird eine Überwachung eingesetzt, aber keine Kontrolle ausgeübt, bezeichnet dies die zweite Form von Schatten-IT, bei der eine IT-Lösung bekannt ist, jedoch bewusst nicht kontrolliert wird (*Monitoring ohne Steuerung*). Manche Unternehmen bezeichnen diese als „Insel-Lösungen“ oder „Small Solutions“ und sehen darin keine Schatten-IT, da Transparenz gewährleistet ist. Kann eine IT-Lösung jedoch nicht überwacht werden, da der technische Zugriff fehlt oder ein IT-System gezielt vom Fachbereich verdeckt eingesetzt wird, zeichnet dies die dritte Form von Schatten-IT aus (*Kein Monitoring möglich*). Die auch „Darkroom IT“ genannte Form wird von manchen Unternehmen nicht mehr als Schatten-IT bezeichnet, da hier die IT-Abteilung keinen Einfluss ausüben kann. Hier gilt es per Governance die Fachbereiche und Mitarbeiter zum Handeln im Interesse des Unternehmens zu bewegen.

<i>Einflußgrad der IT-Abteilung</i>	<i>Bezeichnung</i>	<i>Praxisbeispiel</i>	<i>Ist eine bekannte Schatten-IT Form im Unternehmen bei:</i>
Monitoring mit Steuerung Von der IT-Abteilung verwaltete Lösungen	Managed IT Services	Standard Portfolio Dienstleistungen wie Email oder ERP Systeme oder integrierte anwendergetriebene IT-Lösungen	Nicht Schatten-IT
Monitoring ohne Steuerung Von der IT-Abteilung registrierte Lösungen	Schatten-IT oder Insel-Lösungen	Apple Arbeitsumgebung in der Designabteilung ohne dedizierten Support von der IT-Abteilung	B ¹ , I, J
Ohne Monitoring Von der IT-Abteilung unerkannte Lösungen	Schatten-IT	Anwendergetrieben Skripte, Nutzung von Webservices	A, B ¹ , B ² , C, E, F, G, H, I, J
Kein Monitoring möglich Der IT-Abteilung verborgene Lösungen	Schatten-IT oder Darkroom-IT	Nutzung von externen Services über eine private Datenverbindung oder verdeckte IT-Entwicklung in Fachbereichen	A, C, D, H

Tabelle 2: Monitoring Formen bei Schatten-IT³

Als Schatten-IT werden daher mehrheitlich intransparente IT-Lösungen bezeichnet, während „Insel-Lösungen“ und „Darkroom-IT“ eng verwandte Problemstellungen sind. Für den Betrieb von geschäftskritischen IT-Lösungen streben Unternehmen mindestens die Transparenz einer Insel-Lösungen an. Um Monitoring-Aufwand zu vermeiden, werden unkritische Einzelösungen bewusst als Schatten-IT behandelt.

6 Prozesse, in denen Schatten-IT entsteht

Schatten-IT ist kein plötzlich auftretendes Phänomen, sondern vielmehr das Ergebnis eines Entwicklungsprozesses. Dabei können Transparenz- und Kontrollverlust (wie im vorherigen Kapitel diskutiert) während des gesamten Entwicklungsprozesses einer IT-Lösung auftreten und sich verstärken. Um zu identifizieren, welche Prozesse hiervon betroffen sind haben wir IT-Verantwortliche befragt, in welchen Prozessen Schatten-IT auftritt. Das Ergebnis ist in Tabelle 7 zusammengefasst.

¹ Genannt im Interview mit dem CEO des Unternehmen B

² Genannt im Interview mit dem CIO des Unternehmen B

³ Sortiert und schattiert nach dem Grad des Monitoring und Steuerung von IT-Lösungen

Obwohl die meisten Befragten, in der Nutzung, dem Betrieb und der Entwicklung die typischen Schatten-IT Prozesse sehen, wird mit der häufigen Nennung von externem Sourcing auch der Einfluss von Cloud Computing deutlich. Zusätzlich erkennt man, dass bereits in den frühen Phasen der Lösungsentwicklung (Konzeption und Finanzierung) auf die Entwicklung von Schatten-IT Einfluss genommen werden kann. Anhand dieser Differenzierung der Prozesse kann auch unterschieden werden, ob Schatten-IT generell - inklusive aller potentiellen Vorteile - oder nur der Betrieb und die Nutzung unkontrollierter Lösungen vermieden werden soll.

<i>Prozesse</i>	<i>Relevanz für Schatten-IT</i>	<i>Praxisbeispiel</i>	<i>Kontrollverlust gilt als Schatten-IT bei:</i>
Konzeption	Die Konzeption überführt Geschäftsprozessanforderungen in ein technisches Lösungskonzept. Dieses Lösungskonzept beeinflusst maßgeblich, ob eine interne, externe oder selbst entwickelte IT-Lösung zum Einsatz kommt. Dabei ist die Suche nach vorhandenen internen und externen Lösungen Teil des Prozesses. Die Konzeption gilt im Unternehmen als Schatten-IT, wenn sie ohne Unterstützung durch die IT-Abteilung durchgeführt wird.	Lösungsorientierung anhand von auf dem Markt verfügbaren IT-Dienstleistungen ohne Prüfung des internen Portfolios	A, C, E
Finanzierung	Die Finanzierung stellt transparent (ausgewiesene Kosten) oder intransparent (gezielt verdeckte Kostenstruktur) Geldmittel für das Sourcing, die Entwicklung und den Betrieb von IT-Lösungen bereit. Werden diese ohne Abstimmung mit der IT-Abteilung entschieden, gilt dieses Budget bereits als Form von Schatten-IT.	Von der Fachabteilung finanzierte Softwareentwicklung im Fachbereich.	C, D, E
Externes Sourcing	Das externe Sourcing bezeichnet die Auslagerung der Entwicklung und/oder des Betriebs einer IT-Lösung an ein externes Unternehmen. Wenn das Sourcing ohne Abstimmung mit der IT- und/oder mit der Sourcing-Abteilung im Fachbereich selbstständig durchgeführt wird, stellt dies eine Form der Schatten-IT dar.	Externe IT-Beratung für Fachbereiche; Anwendergetriebener Einkauf von mobilen Geräten	A, C, E, G, H
Interne Entwicklung	Während der Entwicklung wird ein technisches Lösungskonzept innerhalb des Unternehmens in eine betriebsfähige IT-Lösung umgesetzt. Erfolgt diese Entwicklung im Fachbereich ohne Unterstützung der IT-Abteilung spricht man von Schatten-IT.	Anwendergetriebene Entwicklung von Skripten	A, B ¹ , C, E, G, H
Betrieb & Support	Der Betrieb beschreibt die Instandhaltung von IT-Geräten und Systemen und der Support die dazugehörige Anwenderunterstützung und Wartung. Wird beides oder eines von beiden ausserhalb der IT-Abteilung erbracht, gilt dies als Schatten-IT.	Im Fachbereich betriebene Access Datenbank; Betrieb anwendergetriebener mobiler Geräte	B ¹ , C, E, F, G, I
Nutzung	Die Nutzung eines Informationssystems kann auf die Eingabe, Verarbeitung und das Auslesen von Daten reduziert werden. Werden Unternehmensdaten in ein dafür nicht autorisiertes Informationssystem eingegeben, wird dies als Schatten-IT Nutzung bezeichnet.	Nutzung des privaten Emailkontos oder des privaten Rechners für professionelle Zwecke.	A, B ¹ , B ² , C, D, E, F, G, H, I, J

Tabelle 3: Prozesse in denen Schatten-IT entsteht³

7 Potentiale und Herausforderungen von Schatten-IT

Schatten-IT bietet Unternehmen die Möglichkeit, bewusst Freiräume für Mitarbeiter und Fachbereiche zu schaffen, in denen Prozess- und IT-Verbesserung (Innovation) entstehen kann. Gleichzeitig birgt sie aber auch die Gefahr, dass Mitarbeiter der Verantwortung, die mit dieser Freiheit einhergeht, nicht gewachsen sind oder sie ihr nicht bewusst sind. Um herauszufinden, welche konkreten Potentiale und Herausforderungen auftreten, haben wir Un-

¹ Genannt im Interview mit dem CEO des Unternehmen B

² Genannt im Interview mit dem CIO des Unternehmen B

³ Sortiert und schattiert nach der Häufigkeit der Nennung eines Prozesses als Schatten-IT relevant.

ternehmen zu Vor- und Nachteilen von Schatten-IT befragt. Diese sind in Tabelle 4 gegenübergestellt.

Die wichtigsten Vorteile sehen Unternehmen in der kurzzeitigen Verfügbarkeit von Schatten-IT-Lösungen sowie in der mitarbeitergetriebenen Gestaltung ihrer Arbeitsumgebung und neuer IT-Lösungen nach ihren eigenen Anforderungen. Die daraus entstehenden Herausforderungen liegen dabei meist in der Garantie der Datensicherheit, der Verfügbarkeit, des Supports und in der Vermeidung von redundanten IT-Systemen. Als Vorteil erkennen IT-Abteilungen auch die Mitarbeiter-Eigenverantwortung. Dem gegenüber steht das Risiko, dass diese Verantwortung nicht erkannt, angenommen oder sinnvoll eingesetzt wird. Ein weiterer Vorteil ist, dass Schatten-IT-Lösungen mit wenig initialem Aufwand in Betrieb genommen werden können. Hierbei können jedoch unkontrollierte Betriebsstrukturen entstehen, die nur mit hohem Aufwand verwaltet, mit Lizenzen versorgt oder integriert werden können. Als letzten Vorteil erwähnten IT-Verantwortliche den positiven Effekt, dass Schatten-IT als Indikator für nicht erfüllte Anforderungen der Anwender dient, was IT-Abteilungen wiederum zur Verbesserung ihrer Dienstleistungen motiviert.

<i>Potentiale von Schatten-IT</i>	<i>Identifiziert im Gespräch mit:</i>	<i>Herausforderungen von Schatten-IT</i>	<i>Identifiziert im Gespräch mit:</i>
Time to Market Zeitspanne von Auftrag bis Bereitstellung reduzieren	A, C, D, F, G, H, I	Datensicherheit & Compliance Vermeidung von unbefugtem Zugriff auf Unternehmensdaten	A, B ² , C, D, E, F, I
Flexibilität & Produktivität Freiheit der Mitarbeiter, ihre IT-Umgebung optimal auf die Arbeitsprozesse anzupassen	A, B ² , D, E, F, H	Effizienz & Synergien Standardisierung ähnlicher Prozesse, um Skaleneffekte zu erzielen	A, B ² , C, E, F, G, J
Innovation & Prototyping Möglichkeit der Mitarbeiter, mit unterschiedlichen Lösungen zu experimentieren	A, B ¹ , B ² , C, D, I	Kontinuität, Revisionstauglichkeit Garantierte Unterstützung und Nachvollziehbarkeit aller IT-Systeme	A, C, E, F, H, I
Entlastung der IT-Abteilung & Eigenverantwortung Verschiebung von Verantwortungsbereichen von der IT-Abteilung zum Fachbereich	A, B ¹ , F, H, I, J	Kontroll- und Verantwortungsübernahme Bewusste Übernahme von Verantwortung und Haftung für Lösungen im Fachbereich	A, B ² , E, I
Anforderungsmanagement Anwendergetriebene Lösungen erfüllen Anwenderanforderungen genauer	A, B ¹ , C, I, J	Kontrollierte Betriebsstrukturen, Kostentransparenz und Lizenzmanagement Garantierte Skalierbarkeit, Wartbarkeit und ausreichende Lizenzversorgung der IT-Systeme	A, C, H, I, J
Initialkosten Grundgebühr und Bereitstellungskosten	C, D, G, H	Gesamtkosten, Integrationsaufwand und Vendor Lock-In Kosten für langfristigen externen oder internen Betrieb (inkl. Integration)	C, E, F, G, H
Marktvorgleich & Business Relevanz Motivation der IT-Abteilung durch Konkurrenz im Unternehmen durch fremde IT-Anbieter	A, B ¹ , C	Sicherheitsmaßnahmen Freiheit ohne zusätzlichem Sicherheitsaufwand garantieren	B ² , C, I

Tabelle 4: Potentiale und Herausforderungen von Schatten-IT³

¹ Genannt im Interview mit dem CEO des Unternehmen B

² Genannt im Interview mit dem CIO des Unternehmen B

³ Sortiert und schattiert nach der Anzahl von Nennungen der Potentiale von Schatten-IT

Außerdem wird der zusätzliche Aufwand, der bei bewusster Schatten-IT durch ein erweitertes Monitoring entsteht, um die bestehenden Dienstleistungen abzusichern, als Nachteil beschrieben. Es wird deutlich, dass Schatten-IT viele Potentiale bietet, die aus der Eigenverantwortung der Mitarbeiter und dem wachsenden Angebot auf dem IT-Service Markt resultieren. Dabei können intransparente Betriebsstrukturen entstehen, deren Nachteile es zu vermeiden gilt. Um die Potentiale nutzen zu können, müssen daher für die unterschiedlichen Prozessen (siehe Kapitel 6) und technischen Plattformen (siehe Kapitel 4) der Grad an Transparenz, Eigenverantwortung und Kontrolle (siehe Kapitel 5) festgelegt werden.

	Strategie: Risikovermeidung	Strategie: Anwenderorientierung	Strategie: Anwenderverantwortung
Technische Form der Schatten-IT	Anwendergetriebene Innovation (am Beispiel Hardware)		
Unternehmen	C, E, I	A, D, F, G, J	B, H
Zielsetzung	Vermeidung individueller Ausprägungen derselben IT-Lösung, um Supportaufwand zu minimieren	Anpassung der Arbeitsumgebung, um Prozessverbesserung und Individualisierung zu erlauben	Aufwandsreduktion durch mehr Anwender-eigenverantwortung
Steuerungsmethoden	Technische Einschränkungen, Überwachung, Mitarbeitervorschriften, IT Innovation durch Antragswesen	Individualisierung, Meldepflicht, Technische Einschränkungen, Mitarbeitervorschriften	Mitarbeitertraining, Mitarbeitervorschriften, Verantwortungsübergabe, Überwachung
Potentiale	Kostensenkung, Sicherheit	Anwenderproduktivität, Prozessoptimierung	Kostensenkung, Anwenderproduktivität
Herausforderungen	Neubildung von verdeckten dezentralen Schatten-IT-Abteilungen	Support- Sicherheits- und Integrationsaufwand	Trennung von privaten und Unternehmensdaten, Anwenderverantwortung
Technische Form der Schatten-IT	Anwenderverantwortung für Datensicherheit (am Beispiel Software und SaaS)		
Unternehmen	C, D, E, G, H, I, J	A, F	B
Zielsetzung	Vermeidung von Softwareinstallationen und Nutzung von SaaS	Definierte Liste an Software und SaaS für den Privatgebrauch zulassen	Optimale Unterstützung des Anwenders
Steuerungsmethoden	Technische Einschränkungen, Überwachung, Mitarbeitervorschriften	Mitarbeitertraining, Portfolioerweiterung, Mitarbeitervorschriften, Technische Einschränkungen, Überwachung	Mitarbeitertraining, Portfolioerweiterung, Mitarbeitervorschriften, Überwachung
Potentiale	Rechtliche Absicherung, Transparente Datensicherheit	Kontrollierte Individualisierung bei hoher Datensicherheit	Innovation, Individualisierung
Herausforderungen	Eingeschränkte Arbeitsfähigkeit, Verdeckte Schatten-IT: Workarounds	Support- und Sicherheitsaufwand	Inkompatibilität unter Mitarbeitern, Datensicherheit, Mitarbeiterverantwortung

Tabelle 5: Schatten-IT Strategien¹

¹ Je dunkler die Schattierung, desto mehr Unternehmen verwenden diese Strategie

8 Umgangsformen mit Schatten-IT

Um die genannten Vorteile von Schatten-IT zu realisieren und die damit verbundenen Risiken zu minimieren, verfolgen Unternehmen unterschiedliche Strategien. Um diese zu destillieren, wurden IT-Verantwortliche nach ihrer Zielsetzung und Methodik im Umgang mit Schatten-IT befragt. Aus den elf Interviews konnten drei prinzipielle Strategien abgeleitet werden, die anhand der technischen Form individueller Hardware und fremder Software (inkl. SaaS) in Tabelle 5 illustriert werden. Die Strategien lassen deutlich werden, dass Unternehmen im Bereich Hardware bereits versuchen, sich am Anwender zu orientieren. Im Gegensatz dazu setzen IT-Verantwortliche im Softwarebereich auf Risikovermeidung.

9 Zusammenfassung und Ausblick

Dieses Forschungsprojekt hat die in der Praxis auftretenden technischen, organisatorischen und prozessbezogenen Ausprägungen von Schatten-IT identifiziert. Durch die differenzierte Betrachtung können Unternehmen gezielt Potentiale, wie anwendergetriebene Innovation und Prozessverbesserung, nutzen und dabei die Risiken, wie Datensicherheit und Kontinuität des Services, minimieren. Der Schlüssel dabei liegt in den unterschiedlichen Prozessen, in denen Schatten-IT auftreten und sich entwickeln kann. Wird Schatten-IT grundsätzlich verboten, bleiben alle Schatten-IT-Innovationen im Verborgenen und können dadurch die Kommunikation zwischen IT-Abteilung und Fachbereich behindern. Werden jedoch für bestimmte technische (Tabelle 1) und prozessbezogene (Tabelle 3) Bereiche klar definierte Schatten-IT Formen (Tabelle 2) zugelassen, können im Schattenbereich liegende IT-Lösungen erkannt und gegebenenfalls integriert werden. Erste Erfahrungen konnten Unternehmen bereits bei der Unterstützung individueller mobiler Endgeräte sammeln. Einen ähnlichen Weg werden bald auch die primäre Unternehmenshardware (z.B. Notebooks) und zukünftig auch individuelle Softwarelösungen (Softwareinstallationen und SaaS) beschreiten. Mit den vorgestellten Instrumenten können Unternehmen diese Entwicklungen bei Bedarf gezielt einleiten.

Da diese Ergebnisse erst die Formen und die Relevanz von Schatten-IT in Unternehmen identifizieren, ist dies erst die Spitze des Eisbergs. Die Forschung im Themengebiet „Schatten-IT“ am Institut für Wirtschaftsinformatik der Universität St. Gallen wird weiter fortgesetzt. Wie zukünftig die Eigenverantwortung von Anwendern in der IT Governance und Compliance berücksichtigt und wie anwendergetriebene Innovation in Unternehmen entstehen und integriert werden kann, sind aktuelle Forschungsschwerpunkte des Lehrstuhls.

10 Details zur Umfrage: „Umgang mit Schatten-IT“

Es wurden im Zeitraum zwischen 1. Juli und 5. Oktober 2011 elf strukturierte Interviews durchgeführt und dabei die Situation in zehn verschiedenen Schweizer und Deutschen Unternehmen untersucht. Dabei wurden gezielt Unternehmen verschiedener Branchen und Größe ausgewählt. Auf Wunsch der Teilnehmer sind die Ergebnisse der Umfrage anonymisiert worden. Tabelle 6 und Tabelle 7 zeigen die Charakteristika der befragten Organisationen.

	Unternehmen A	Unternehmen B	Unternehmen C	Unternehmen D	Unternehmen E
Interview-partner	CIO	CEO und CIO	COO	CIO	CIO
IT-Abteilung	Zentrale IT	Dezentrale IT	Zentrale IT	Zentrale IT	Zentrale IT
Betriebsform	Öffentlich	Öffentlich	Privat	Öffentlich	Privat
Branche	Behörde	Forschung & Beratung	Bank	Bank	Automobil
Gewinnmarge	ohne Gewinnmarge	Hohe Gewinnmarge auf niedrige Stückzahlen	Niedrige Gewinnmarge auf hohe Stückzahlen	Niedrige Gewinnmarge auf hohe Stückzahlen	Niedrige Gewinnmarge auf hohe Stückzahlen
IT Anwender	2500	150	650	5000	60000
IT Mitarbeiter	45	3	50	840	750
IT Budget	25 Mio. CHF	keine Angabe	60 Mio. EUR	keine Angabe	keine Angabe

Tabelle 6: Liste der Interviewpartner Teil 1

	Unternehmen F	Unternehmen G	Unternehmen H	Unternehmen I	Unternehmen J
Interview-partner	CIO	CIO	CIO	CIO	CIO
IT-Abteilung	Zentrale IT	Zentrale IT	Zentrale IT Entwicklung	Zentrale IT	Zentrale IT
Betriebsform	Privat	Privat	Privat	Privat	Privat
Branche	Maschinenbau	Versicherung	Bank	Automobil	Beratung
Gewinnmarge	keine Angabe	Gemischt	Niedrige Gewinnmarge auf hohe Stückzahlen	Hohe Gewinnmarge auf niedrige Stückzahlen	Niedrige Gewinnmarge auf hohe Stückzahlen
IT Anwender	16000	7200	22000	1800	4000
IT Mitarbeiter	350	720	2500	60	110
IT Budget	keine Angabe	200 Mio. CHF	700 Mio. CHF	20 Mio. EUR	keine Angabe

Tabelle 7: Liste der Interviewpartner Teil 2

11 Literaturverzeichnis

- Escherich, M. (2011). *Search Analytics Trends: The Inevitable Consumerization of Corporate IT*. Gartner (pp. 1-5). Retrieved from <http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&id=1591515&ref=>
- Gens, F., Levitas, D., & Segal, R. (2011). *Consumerization of IT Study: Closing the “Consumerization Gap.”* Framingham. Retrieved from <http://www.unisys.com/iview>
- Global Survey: Has Cloud Computing Matured?* (2011). *Avanade Research & Insights* (pp. 1-13). Retrieved from [http://www.avanade.com/Documents/Research and Insights/Global_Survey_Slide_Graphics_Has_Cloud_Matured.pdf](http://www.avanade.com/Documents/Research%20and%20Insights/Global_Survey_Slide_Graphics_Has_Cloud_Matured.pdf)
- Holmes, A. (2008). *Commoditization and the Strategic Response* (pp. 1-245). Gower. Retrieved from <http://www.ebookmall.com/ebook-club.htm>
- Meeker, M., Devitt, S., & Wu, L. (2010). *Internet Trends*. Morgan Stanley (pp. 1-87).
- Meeker, M., Flannery, S., Dawson, J., Ji, R., Huberty, K., Delfas, N., Tanaka, H., et al. (2009). *The Mobile Internet Report*. Morgan Stanley (pp. 1-424). Retrieved from http://www.morganstanley.com/institutional/techresearch/pdfs/mobile_internet_report.pdf
- RSA Security Inc. (2007). *The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk* (pp. 1-12). Bedford, MA (USA). Retrieved from <http://www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf>
- Schüler, P. (2011, September). Mitbringsel - Strategien für den sicheren Firmenzugang mit privaten Handys. *heise mobil*, 1-9. Retrieved from <http://www.heise.de/mobil/artikel/Strategien-fuer-den-sicheren-Firmenzugang-mit-privaten-Handys-1344853.html>
- Zeitler, N. (2011). Forscher: CIOs scheuen den Konflikt. Tabu-Thema Schatten-IT. *CIO.com*. Retrieved from <http://www.cio.de/strategien/2273381/index.html>
- Zimmermann, S., Rentrop, C., & Laak, O. van. (2011). IT-Problemfeld: Service Management und Schatten-IT. *IT Management*, 9, 1-6. Retrieved from <http://www.it-daily.net/content/view/4645/30/>