Chancen und Risiken im Umgang mit der Schatten-IT

Der Begriff Schatten-IT ist negativ belegt und existiert in keiner IT-Strategie – dennoch wächst die Schatten-IT stetig. Erreicht sie bezüglich Kosten oder Wichtigkeit eine kritische Grösse, tauchen entsprechende technische und organisatorische Probleme auf, die dann ungeplanten Mehraufwand verursachen. Hannes Lubich

Hannes Lubich

Der Begriff «Schatten-IT» beschreibt informationstechnische Systeme, Prozesse und Organisations¬einheiten, die in den Fachabteilungen eines Unternehmens neben der offiziellen IT-Infrastruktur und ohne das Wissen des IT-Bereichs angesiedelt sind (Definition Wikipedia). Eine Schatten-IT wird also – aufgrund unbefriedigter Bedürfnisse der Benutzer – in Eigenregie beschafft und betrieben, wobei die Integration in die Unternehmens-IT und die IT-Prozesse für Beschaffung, Wartung, Überwachung etc. nicht berücksichtigt werden. Die Ursachen hierfür sind vielfältig:

1. «plug & play» Installationen bezüglich Hardware und Software – die IT erscheint insbesondere den «digital natives» weniger abschreckend, da viele Endbenutzer komplexe Heim-IT-Umgebungen betreiben.

2. Die IT hat über entsprechende Produkte viel Verantwortung an ihre Endbenutzer ausgelagert. Es ist kein Zufall, dass sich in vielen Unternehmen als Gegenreaktion Remote-Desktop-Lösungen etablieren, um die völlige Konfigurationsfreiheit der Endbenutzer einzuschränken.

3. Die IT ist ein bequemes Ziel für Unzufriedenheit und Kostendruck, weil in jeder Firma die IT zwischen Kundenfokus und «economy of scale» hin- und hergerissen ist und daher im Sinne eines sinnvollen Durchschnitts meist eine Nutzergruppe weniger gut unterstützt, als eine andere.

4. Mitarbeitende sind mit der Unternehmens-IT tendenziell unzufrieden – basierend auf einer Mischung aus falscher Erwartungshaltung, sicherheitsbedingen Einschränkungen, wenig Transparenz über Kosten und Aufwände, wachsendem Spar-/ Effizienzdruck sowie wenig Selbstdisziplin in der Führung (oft sind es leitende Mit¬arbeitende, die unter Missachtung definierter Prozesse die Integration ihres Lieblings-«Gadgets» fordern).

5. Über die Unternehmens-IT redet man oft nur im Negativ-Fall – das neueste Privatgerät ist im Vergleich zu den «langweiligen» Systemen und Diensten der Unternehmens-IT meist etwas Positives (bis es zum ersten Mal Probleme verursacht).

Einfluss aktueller IT-Trends

Einige aktuelle technische IT-Trends verschärfen das Problem noch weiter:

- Das wachsende Angebot performanter und günstiger Cloud-Dienste erlaubt die rasche Ausla¬gerung von Diensten bzw. deren Aufbau, ohne dass das Unternehmen davon Kenntnis hat, insbesondere wenn der Zugang über etablierte Protokolle wie HTTP erfolgt.
- Der Wunsch nach der Integration privater Endgeräte («bring your own device») führt zu komplexen Abklärungen zu Integration, Einfluss auf die IT-Prozesse, rechtlichen Konsequenzen usw. Viele Anwender wollen dies nicht abwarten. Da diese Geräte jedoch eigene IT-Dienstleistungen umfassen (Hersteller-Clouds, private Softwarelizenzen etc.), gilt hier eher «bring your own infrastructure» oder «bring your own data center», was die Integration nicht vereinfacht.
- Der mobile IT-Markt wird von schnelllebigen, performanten Endgeräten mit schneller und flächendeckender Netzanbindung überschwemmt – damit steigt der Druck, immer neue Geräte, Betriebssysteme und Anwendungen rasch in die Unternehmens-IT zu integrieren. Diesem Erwartungsdruck kann die Unternehmens-IT meist nicht standhalten.

Durch die Verfügbarkeit dieser Dienste und Ausrüstung sowie durch die Anforderungen der externen Unternehmenskunden steigt zudem der Druck auf die Mitarbeitenden, jederzeit ortsunabhängig mit voller Funktionalität auf die Unternehmensdaten und -anwendungen zugreifen zu können.

Risiken einer Schatten-IT

Aus dem Einsatz einer Schatten-IT im Unternehmen ergeben sich Kosten und Risiken, deren typischste Vertreter im Folgenden diskutiert werden.

Technologische Risiken

Aus Sicht der Technologie entstehen durch die Existenz einer Schatten-IT wesentliche Risiken, da häufig

- ungetestete, ggf. unsichere IT-Komponenten eingesetzt werden, die oft nicht für den Einsatz im Unternehmensumfeld entwickelt wurden,
- die Speicherung und Bearbeitung sensitiver Daten ausserhalb der Kontrolle der Unternehmung und ihres Sicherheitsdispositives liegen,
- Mitarbeitende «ihre» Geräte und externen Dienste (und damit meist auch die Daten) beim Austritt mitnehmen und
- bei technischen Ausfällen und Betriebsunterbrüchen

(z.B. wegen Sicherheitsvorfällen, physischen Schäden usw.) keine Betriebsweiterführung gewährleistet werden kann.

Prozessbezogene Risiken

Über die technologischen Risiken hinaus entstehen durch eine Schatten-IT weitere Risiken bezüglich der etablierten Unternehmens- und IT-Prozesse:

- Der Aufwand für Aufbau und Pflege der IT-Unternehmensarchitektur (mit dem Ziel der Vereinfachung, Skalierbarkeit, etc.) wird weitgehend wertlos.
- Definierte Prozesse mit zugeordneten Service Agreements können nicht mehr bezüglich Dienst¬güte gemessen werden – Führungskennzahlen bezüglich Qualität, Quantität und Funktionalität durch die IT verlieren ihre Aussagekraft.
- Etablierte, geschäftsrelevante Abläufe (Stellvertretung, Mehraugenprinzip, Nachvollziehbarkeit etc.) können nicht mehr Ende-zu-Ende abgewickelt und überwacht werden – die erzielten Ergebnisse werden somit zufällig und nicht mehr vorhersagbar.

Geschäftliche und Führungsrisiken

Von den prozessbezogenen Risiken ist es nur noch ein kleiner Schritt zu Risiken, welche die Geschäftsausübung und «corporate governance» tangieren:

- Da die IT umgangen wird, kann sie ihre Verantwortung für die Geschäftsunterstützung nicht wahrnehmen – zudem kann sie ihren Nutzen und Beitrag zum Geschäftserfolg nicht mehr nachweisen. Die «economy of scale» geht verloren und die IT wird zum Kandidaten für eine umfassende Auslagerung.
- Es besteht die akute Gefahr der Nicht-Einhaltung rechtlicher oder regulatorischer Vorschriften mit diversen Folgerisiken, auch in nicht regulierten Märkten (zum Beispiel bezüglich geschäftlicher Nutzung von Software, die nur für die Nutzung im Privatgebrauch lizenziert wurde).
- Da der Betrieb der Schatten-IT nicht offiziell unterstützt wird, sondern «best effort» als Zusatzleistung erfolgt, kann es zu kritischen Abhängigkeiten von Einzelpersonen kommen. Zudem steigt das Überlastungs-Risiko für die Betroffenen stark an.

Chancen einer Schatten-IT

Angesichts dieser Risiken müsste jegliche Schatten-IT sofort eingesammelt und deaktiviert werden. Jedoch bietet eine Schatten-IT auch offensichtliche Vorteile.

Technologische Chancen

Bezüglich Technologie-Einsatz bietet eine Schatten-IT erhebliche Vorteile gegenüber der etablierten Unternehmens-IT:

- «State of the art» Technologie bietet eine Vielzahl neuer Funktionen, die die Produktivität der Mitarbeitenden positiv beeinflussen können, während die offizielle, oft (zu) stark standardisierte IT den Durchschnitt aller Anforderungen abdecken muss und so niemanden wirklich befriedigt.
- Eine für einen bestimmten Zweck aufgebaute IT erlaubt eine raschere «time to market» für innovative oder explorative Lösungen für den Endkunden, der solche Dienste zunehmend auch erwartet.

Prozessbezogene Chancen

Aufbauend auf den technologischen Chancen können auch Abläufe im Unternehmen durchaus von der Existenz einer Schatten-IT profitieren:

- Dichter an den Anforderungen der internen oder externen Kunden kann man nicht sein.
- Liegt die operative und «profit & loss»-Verantwortung für eine Schatten-IT beim internen Betreiber, kann sich die Unternehmens-IT auf die effiziente Erbringung weniger wohldefinierter Basisdienste konzentrieren.
- Die Skalierung und Rückverrechnung der IT-Kosten kann dynamischer und kunden-/projektbezogener erfolgen.

Geschäftliche und führungsbezogene Chancen

Schliesslich kann auch die Geschäftsausübung und -ausdehnung von einer anwendernahen IT profitieren:

- Eine kundennahe IT kann ein differenzierender Marktfaktor sein - die Erwartung der externen Kunden (insbesondere der «digital natives») wird besser adressiert.
- Das kreative Potential der jungen, technologieaffinen Generation als potentielle Mitarbeitende wird besser genutzt – das Unternehmen bleibt angesichts des Fachkräftemangels attraktiv.

Umgang mit einer Schatten-IT

Natürlich gibt es im Spannungsfeld zwischen Kundennähe und Standardisierungsdruck kein Standardrezept, welches den richtigen Umgang mit der Schatten-IT aufzeigt. Jedoch kann ein Vorgehensplan helfen, Chancen und Risiken zu erkennen, abzuwägen und zu adressieren.

Ein grober Vorgehensplan enthält die folgenden Phasen:

Erkennung: Die Existenz der Schatten-IT ist offiziell bekannt, Probleme, Vorteile und Nachteile werden transparent, die Verantwortlichen legen Kosten/Nutzen und Risiken/Chancen offen.

Akzeptanz: Es wird eine klare Strategie festgelegt und offen kommuniziert – dies beinhaltet auch den Willen zur Umsetzung und Sanktionierung unerwünschter Abweichungen. Dabei kann es Teilbereiche im Unternehmen geben, die eine «user empowered IT» einsetzen (mit Delegation von Verantwortung und Kompetenz). Eine Umbenennung (also weg von der «Schatten-IT») kann schon ein einfaches Mittel sein, Akzeptanz zu schaffen.

Langfristige Umsetzung: Aus der bisherigen Schatten-IT werden Lehren bezüglich Einsatz und Nutzen gezogen, die die offizielle IT attraktiv und kundennäher positionieren. IT ist noch lange keine «Commodity», weil die ständige Erneuerung und Innovation der IT dies verhindert. Die offizielle IT muss agil und fähig sein, neue Anforderungen so rasch zu integrieren, dass die Schatten-IT klein bleibt beziehungsweise keine wesentlichen Vorteile bietet.

Fazit

Agile Unternehmen, welche die Existenz ihrer Schatten-IT anerkennen, diese in ihre kommunizierte IT-Strategie integrieren und wo sinnvoll in eine akzeptierte «user empowered IT» umwandeln, werden tendenziell stärker von den Chancen profitieren, als unter den nicht vermeidbaren Risiken leiden.

Prof. Dr. Hannes P. Lubich, Institut für Mobile und Verteilte Systeme, Fachhochschule Nordwestschweiz, Brugg / Windisch, hannes.lubich@fhnw.ch