



Das Phänomen Schatten-IT

Wenn gute Absichten plötzlich zum Problem werden



facebook dropbox

Kontaktieren Sie uns:

Carsten Graf

+49 89 416 1169 40

<https://www.code42.com/de/>



Inhalt

1. Einleitung
2. Was sind die Ursachen der Schatten-IT – was motiviert den Anwender?
3. Die eigentlichen Gefahren
4. Vorbeugen durch Aufklärung
5. Alternative Lösungen
6. Fazit

Appendix

7. Haftungsfragen und Lösungsansätze im Hinblick auf die EU-DSGVO



Vorwort von Rainer Fahs (Chairman der EICAR)

Schatten-IT ist weniger ein Problem auf technischer, sondern auf organisatorischer Ebene. Es geht dabei nicht unbedingt darum, dass ein Angreifer Malware einsetzt, um einen Schaden anzurichten oder eine Website mit DDoS-Attacken kolportiert. Schatten-IT ist vielmehr eine Konsequenz aus der gesellschaftlichen Veränderung, der digitalen Transformation und einem sich verändernden Verhalten im Umgang mit Informationen. Dennoch bedeutet sie ein nicht zu unterschätzendes Risiko für Unternehmen. In dem Moment wo eine IT-Abteilung die Kontrolle über die Geschäftsabläufe verliert kann eine gewisse Datenintegrität nämlich nicht mehr gewährleistet werden.

Deshalb beschäftigt sich die EICAR in diesem Positionspapier mit den Ursachen und Gefahren und gibt im Anschluss einige Verhaltenstipps für IT-Verantwortliche.

Rainer Fahs
EICAR Chairman





Vorwort von Carsten Graf (Managing Director DACH bei Code42)

Informationen sind das Fundament und der Motor für Geschäftserfolg im digitalen Zeitalter, daher sind Schutz und lückenlose Sichtbarkeit von Daten, ihre Absicherung für den Ernstfall über das Datenzentrum hinaus und der gewissenhafte Umgang mit ihnen eine absolute Priorität. Gerade Endgeräte, auf denen das Gros an Informationen erstellt und verarbeitet werden, sind hier im Brennpunkt und sollten keinesfalls der unternehmensweiten Backup & Recovery-Strategie vernachlässigt werden. Dennoch haben wir in der aktuellen „CRTL-Z“-Studie von Code42 erfahren, dass drei Viertel der Entscheider in Unternehmen beruflich Services nutzen, die weder mit den Sicherheits- und Compliance-Richtlinien des Unternehmens übereinstimmen, noch von der IT umfassend überwacht und abgesichert werden können. Laut der Studie ist gleichzeitig einem Großteil davon durchaus bewusst, dass nicht freigegebene Anwendungen ein immenses Risiko darstellen und Datenverlust verheerende Auswirkungen auf Image und Geschäft haben kann. Dieses Paradox macht deutlich, dass Schatten-IT und ihre Risiken durchaus ein Thema auf allen Unternehmensebenen, die Sensibilisierung für zielführende Lösungsansätze jedoch noch stark ausbaufähig ist.

Daher haben wir gemeinsam mit der EICAR und den Rechtsexperten von Cyberlegal diesen umfassenden Leitfaden für Unternehmen zusammengestellt. Er gibt Ihnen einen tiefen Einblick in Ursachen, Risiken und praktikable Lösungen, um die Herausforderung Schatten-IT nachhaltig zu meistern.

Carsten Graf
Managing Director DACH bei Code42





1. Einleitung

Derzeit ist Schatten-IT in aller Munde – die Fachpresse berichtet regelmäßig und in den Unternehmen wird Schatten-IT bereits im Tagesgeschäft „gelebt“ – zumeist jedoch unwissend.

Der Begriff Schatten-IT steht dabei für IT-Anwendungen, die in Organisationen genutzt werden, ohne in die eigentliche IT-Landschaft eingebettet zu sein – sprich es werden Systeme und/oder Software durch Abteilungen oder einzelne Mitarbeiter parallel zur offiziellen IT-Infrastruktur genutzt. In der Regel ist diese Nutzung auch nicht von der IT-Abteilung genehmigt worden.

Für die unternehmensinternen IT-Abteilungen ist dieser unkontrollierte Wildwuchs natürlich ein Alptraum – wenn unbemerkt Hard- und Software genutzt wird, die nicht den gleichen Sicherheitsrichtlinien unterliegen, wie die offiziell im Unternehmen eingesetzten Technologien.

Ein moderner Mitarbeiter, der zur Generation Y gehört, mag jetzt vielleicht denken, dass dies heutzutage doch kein Problem mehr darstellen dürfte. Da geht Usability, Produktivität und Funktionalität doch eindeutig vor. Außerdem, so ein vielgehörter Satz, sei doch die interne IT viel zu unflexibel, um die Bedürfnisse der Fachabteilungen schnell umzusetzen. Hier prallen die Meinungen von Fachabteilungen und IT aufeinander: Auf der einen Seite der Wunsch nach Flexibilität und einem Plus an Produktivität – auf der anderen Seite die Anforderung an größtmögliche Sicherheit und Verwaltbarkeit innerhalb eines oft sportlichen Budgetrahmens.

EINLEITUNG

Doch gibt es noch einen weiteren Widerspruch, der auch die abteilungsübergreifende Kommunikation deutlich erschwert: Aus organisatorischer Sicht und insbesondere aus Gründen der Unternehmens-Policy liegt natürlich ein klares Fehlverhalten vor, wenn ein Mitarbeiter aus Gründen der mangelnden Produktivität oder gar Funktionalität an der bestehenden IT-Infrastruktur vorbei arbeitet.

Aber handelt der Mitarbeitende nicht auch irgendwo im Sinne des Arbeitgebers, wenn seine Motivation eine rasche Umsetzung der Arbeitsschritte auf reibungslose Art und Weise ist? Ist der Fehler also beim Mitarbeitenden zu suchen oder stößt die IT-Abteilung schlicht und ergreifend an ihre Grenzen, was digitale Transformation angeht?

Wo liegt der FEHLER?





2. Was sind die Ursachen für Schatten-IT – Was motiviert die Anwender?

Schatten-IT scheint insbesondere im Kontext Cloud-Computing weit verbreitet. Das belegt die Skyhigh-Studie "Cloud Adaption & Risk Report" Q1 2015. Danach kommen in Unternehmen durchschnittlich 738 Cloud-Dienste zum Einsatz, aber nur weniger als ein Zehntel davon sind bei der IT-Abteilung bekannt und genehmigt. 82 Prozent der befragten Mitarbeiter gaben gegenüber Skyhigh zu, inoffizielle Cloud-Apps zu nutzen. Als Hauptgründe nannten sie die Vertrautheit mit den betreffenden Anwendungen aus dem Privatgebrauch sowie langwierige Genehmigungsverfahren in der jeweiligen IT-Abteilung. Somit werden auch sämtliche Service Level Agreements umgangen, die durch die IT-Abteilung gewährleistet werden – ein effizienter und zuverlässiger IT-Support scheint damit gefährdet.

Das Phänomen ist bei den IT-Verantwortlichen jedoch bereits angekommen. Aus technischer Sicht scheint der einzig sinnvolle Schritt eine Modernisierung der IT-Infrastruktur. Und organisatorisch können nur Mitarbeiterschulungen, die gezielt für eine erhöhte Sensibilisierung sorgen, helfen.

Die digitale Transformation bezieht sich keinesfalls nur auf die IT-Abteilung. Fälschlicherweise liegt der Verdacht nahe, es müsse sich doch um irgendwelche Softwarelösungen handeln, die Unternehmensabläufe einfach nur digitalisieren. Im World Wide Web ist längst schon ein Kampf der Innovationen entfacht. Neue Apps für das Smartphone herzustellen galt vor nicht allzu langer Zeit noch als Paradedisziplin und ist doch längst schon zu Commodity geworden. Nehmen wir einmal beispielhaft Marketingabteilungen. Sie stehen unter Druck mit eingeschränkteren Budgets immer noch mehr Leads für den Vertrieb zu generieren. Mit weniger Budget? Logo, da wird ja auch längst nicht mehr in teure Anzeigenkampagnen oder Agenturleistungen investiert. Nein ganz im Gegenteil! Im Zeitalter der digitalen Transformation steht unter dem Zeichen der Marketing Automatisierung – soll ja schließlich Zeit und Geld sparen.

URSACHEN

Technische
Möglichkeiten

The background image shows a man in a grey suit and white shirt holding a white tablet. Overlaid on the image is a conceptual diagram with a central orange text 'SCHATTEN IT URSACHEN' and four surrounding grey boxes with white text: 'Technische Möglichkeiten' (top-left), 'Umsetzungs-Anforderung' (top-right), 'Fertigkeiten des Anwenders' (bottom-left), and 'Informations-Verhalten' (bottom-right). Thin white lines connect the central text to each of the four boxes. The word 'URSACHEN' is also visible in large, faint letters at the bottom left of the image.

Umsetzungs-
Anforderung

SCHATTEN IT
URSACHEN

Fertigkeiten des
Anwenders

Informations-
Verhalten

Außerdem sind Marketing- und Vertriebsabteilungen voll und ganz auf den Hype „Customer Centricity“ fokussiert. Sprich es gilt aus dem Berg an „Big Data“ jene Informationen zu extrahieren, die einen fundierten Einblick in das Kaufverhalten der Zielgruppe geben. Und an dieser Stelle entsteht auch schon das ganze Dilemma. Die Marketingabteilungen tun vermeintlich nichts „Böses“, sondern handeln im Sinne der Effizienz sozusagen im guten Glauben. Seien es Analyse-Tools, Werkzeuge zur Marketing-Automation oder ganz banale Filesharing Tools. Die Nutzung ist nur ein paar Mausklicks und eine Kreditkartennummer entfernt. Und die IT-Abteilungen können dieser Entwicklung kaum noch standhalten. Sie haben zumeist gar keine Ahnung davon, was in der Marketingabteilung vor sich geht. Und dem Marketeer wäre es ohnehin ein echtes Rätsel, warum er darüber, dass er seinen Job richtig und gut mache, auch noch die IT informieren sollte?

Langer Rede kurzer Sinn, die technischen Möglichkeiten im Informationsumgang haben derzeit einen Stand erreicht, wo es zur echten Herausforderung wird, dem Tempo noch Stand zu halten. Die technischen Möglichkeiten scheinen also grenzenlos und werden damit zu einer Ursache für Schatten-IT.

Ein anderes Thema ist das Informationsverhalten selbst, das sich in den letzten Jahren immens verändert hat. Wenn man sich allein die Datenvolumina anschaut, die Server mittlerweile zu verarbeiten im Stande sind. Hat man vor nicht allzu langer Zeit noch Festplatten mit 5 GB beim Elektrofachhandel kaufen können, bewegen wir uns mittlerweile in Terrabyte-Größen. Und wenn der Anwender erst einmal in den Genuss gekommen ist, den technischen Möglichkeiten bieten, will er darauf logischerweise nicht mehr verzichten.



Nicht nur aus privaten Interessen, sondern insbesondere auch aus beruflichen. Einmal angenommen, die interne Marketing-Abteilung eines großen Unternehmens ist gerade mit der Anfertigung einer Image-Broschüre bzw. einem Produktlaunch beauftragt.

Die Texte sind geschrieben, die Bilder geschossen und ausgewählt – nun müssen nur noch die einzelnen Elemente zusammengefügt werden. Die Übermittlung der Texte ist recht einfach, da diese meist wenig Speicherplatz benötigen und somit über die gängigen E-Mail-Programme versendet werden können. Etwas herausfordernder gestaltet sich die Versendung des Bildmaterials, das in der Regel für den Druck hochaufgelöst sein muss. Eine Möglichkeit ist, die mehrere Megabyte großen Dateien einzeln per Mail zu übermitteln. Das ist teilweise sehr störanfällig und zeitaufwendig. Daher greifen die Nutzer oftmals auf komfortablere Methoden zurück, die sie aus ihrem Alltagsleben kennen, deren Nutzung sie gewohnt sind und die sie beherrschen: sie installieren zum Beispiel den Filesharing-Dienst Dropbox auf ihrem Arbeitsplatzrechner und tauschen darüber die Daten aus.

Wo lauern die Gefahren?

Das mag auf den ersten Blick zwar zweckmäßig sein, ist aber ein Horrorszenario für jedes Unternehmen! Denn ein fremder Nutzer, der sich auch noch außerhalb des gesicherten Unternehmensnetzwerkes befindet, erhält Zugriff auf einen Rechner innerhalb des geschützten Bereiches. Dort dann Schadsoftware einzuschmuggeln, ist ziemlich leicht.

Die Nutzung von Filesharing-Diensten verursacht noch ein weiteres Gefahrenszenario: der Sender übermittelt seine Daten zunächst verschlüsselt an den Dienstleister.



URSA

Dieser wiederum entschlüsselt die Daten auf seinem eigenen Server und verschlüsselt diese dann wieder für den Versand zum Empfänger. Diese Vorgehensweise eröffnet einen hervorragenden Weg für Cyber-Kriminelle, um während der Umwandlung die im Klartext vorliegenden Daten auf dem Server des Dienstleisters abzugreifen. Auf diese Weise sollen schon Entwürfe von Kollektionen bekannter Designer ausspioniert worden und in die Hände von Mitbewerbern gelangt sein.

Das Thema Umsetzungsanforderungen ist mit dem erhöhten Druck bei reduzierten Budgets zu erklären. Den Fachabteilungen bleibt nämlich oft weniger Zeit bei der Umsetzung ihrer Aktivitäten. Das Thema Budget-Reduktion spielt in diesem Zusammenhang eine ähnlich gewichtige Rolle. Sprich „doing more for less“ zieht sich durch sämtliche Abteilungen durch. Es stellt sich an dieser Stelle aber wieder die Frage, inwieweit die Vorwurfsvermutung gilt, sofern sich eine Abteilung Werkzeugen aus dem Netz bedient, die entsprechende Arbeitserleichterungen bringen.



Eine weitere Ursache für das Phänomen ist gleichsam ein sehr interessantes: die Generation Y oder auch Millennials genannt. Sie bilden mittlerweile eine wichtige Berufsgruppe. Diese „Digital Natives“ sind mit dem Internet, sozialen Medien und mobilen Endgeräten groß geworden. Nicht nur aus der Macht der Gewohnheit übernehmen sie nun die Verhaltensmuster ins Berufsleben. Für diese Generation gehört der Umgang mit Informationen zum Lifestyle. Sie postulieren in Unternehmen eine „always on“ Attitude und sind daher auch nicht in klassische Unternehmens-Policies hineinzuzwängen. Und da die Millennials technisch auch noch überaus affin sind, weichen sie sehr schnell auf alternative Kommunikationskanäle und -plattformen aus, sobald die Unternehmens-IT an ihre Grenzen stößt. Ein weiterer Punkt in diesem Zusammenhang ist sicher das Verständnis- und Kommunikationsproblem zwischen Tradition und Moderne – einer klassisch geprägten IT-Abteilung mit klaren Regeln und starren Vorschriften und einer agilen und „freiheitsliebenden“ neuen Generation. Da scheint es nur logisch, dass die Millennials oft ein Eigenleben entwickeln, das den Einsatz von alternativen Arbeitsmitteln und Anwendungen einschließt. Hier würde es sich mit Sicherheit anbieten, wenn sich die IT-Abteilungen künftig mehr in die Rolle eines Dienstleisters, sozusagen eines Enablers, versetzen und proaktiv auf die Anforderungen und Sorgen der Fachabteilungen eingehen würden.



3. Die eigentlichen Gefahren

Am 25. Juli 2015 ist das viel diskutierte IT-Sicherheitsgesetz in Kraft getreten. Kurz zusammengefasst soll es dazu beitragen, dass wichtige und kritische Infrastrukturen besser vor digitalen Angriffen geschützt werden. Das Gesetz gilt für Betreiber von Webangeboten wie Onlineshops, Telekommunikationsunternehmen, Banken, Energieversorger, Wasserwerke oder Krankenhäuser – welche Unternehmen dem Gesetz genau unterliegen, wird über eine noch zu verabschiedende Rechtsverordnung geregelt werden. Insgesamt gelten aber nun höhere Anforderungen in Sachen IT-Sicherheit und Datenschutz. IT-Sicherheitsvorfälle müssen – wie es heute schon für Kernkraftwerke und Telekommunikationsanbieter gilt – gemeldet werden. Setzen dies Unternehmen nicht um, drohen empfindliche Bußgelder.

Damit fügt sich dem Reigen von Compliance-Anforderungen an deutsche Unternehmen eine weitere Komponente hinzu, die Regelungsdichte nimmt zu. Darüber hinaus beschäftigt sich die deutsche Rechtsprechung zunehmend mit Fragen der Haftung von Management und Aufsichtsorganen. Hier immer sämtliche Fallstricke auf dem Schirm zu haben, ist für Unternehmen eine echte Herausforderung. Es kann durchaus sein, dass Unternehmen ahnungslos gegen Regeln verstoßen. Aber auch hier gilt der Grundsatz: „Unwissenheit schützt vor Strafe nicht“. Nehmen wir doch einmal das Beispiel der riskanten Nutzung des Filehosting-Dienstes Dropbox oder anderer Freeware zum Austausch großer Datenmengen.



Mitarbeiter nutzen diese Dienste meist, weil sie sie aus der privaten Nutzung kennen und weil sie keinen zeitraubenden Beschaffungsprozess anstoßen wollen. Dennoch nehmen sie damit in Kauf, dass dadurch Sicherheitslücken im Unternehmen entstehen, die durch IT-Abteilungen meist nur schwer entdeckt und geschlossen werden können. Damit landen eventuell auch vertrauliche oder unter das Datenschutzgesetz fallende sensible Daten beim Cloud-Anbieter, wenn die Daten nicht zusätzlich verschlüsselt werden. Spätestens wenn Daten dadurch verloren gehen, besteht ein Rechtsproblem.

Prinzipiell ist das Unternehmen für die ordnungsgemäße Verarbeitung von personenbezogenen Daten verantwortlich und muss deshalb – im Rahmen des Risikomanagements – entsprechende Vorkehrungen treffen. Je nach Organisationsstruktur haften die Geschäftsführung, der Finanzvorstand, der CIO oder der Compliance-Verantwortliche unter Umständen sogar persönlich für Vorfälle.

Unwissenheit schützt **NICHT!**

Der BGH hat beispielsweise in einer Entscheidung (BGH 5 StR 394/08) folgendes zum Pflichtenkreis eines Compliance Officers erklärt: „Deren Aufgabengebiet ist die Verhinderung von Rechtsverstößen, insbesondere auch von Straftaten, die aus dem Unternehmen heraus begangen werden und diesem erheblichen Nachteil durch Haftungsrisiko oder Ansehensverlust bringen können.“

„Diese strafrechtliche Relevanz ist auch auf das Zivilrecht übertragbar. Sprich: jedem Compliance-Officer kann hier Regress drohen.“



Zivilrechtliche Haftungsgefahren können durch eine sogenannte D&O-Versicherung abgesichert werden, vor strafrechtlicher Verfolgung schützt die allerdings nicht. Eine Umfrage des FINANCE Magazins bei CFOs hat ergeben, dass immerhin 44 Prozent der Finanzchefs beunruhigt sind, als CFO persönlich zu haften.

Aber gilt das auch, wenn Geschäftsführer, Finanzvorstand oder Compliance Officer von einer Rechtsverletzung schlicht und ergreifend nichts wissen? Wie erwähnt: Unwissenheit entschuldigt nicht. Und gerade deshalb müsste das Thema Schatten-IT bei Entscheidern ganz oben auf der Agenda stehen.



Vor allem in drei Bereichen bedeutet Schatten-IT Gefahr im Verzug:

1. Datenschutz: Wenn wir beim Beispiel Datenübertragung durch Cloud Services bleiben, muss der CIO beachten, dass hier nach §11 Bundesdatenschutzgesetz (BDSG) eine Auftragsdatenverarbeitung vorliegt. Der unbemerkt benutzte Cloud-Service-Anbieter ist damit als verlängerter Arm des Unternehmens tätig. Dennoch bleibt das Unternehmen aber die verantwortliche Instanz für die Daten. Gehen auf diesem Wege etwa personenbezogene Mitarbeiter- und/oder Kundendaten verloren, haftet das Unternehmen.

2. Datensicherheit: Gerade das IT-Sicherheitsgesetz regelt unter anderem, dass Unternehmen ihre IT-Strukturen vor Cyberangriffen schützen und dabei zumindest Mindeststandards berücksichtigen müssen. Solche Standards für die Beschaffung von Hard- und Software bieten beispielsweise die DIN-Normen der ISO/IEC 20000 und 27000er-Reihe. Schatten-IT kann solche Bestrebungen im Unternehmen unterlaufen.

3. Lizenzmanagement: Die Softwarebeschaffung und das Lizenzmanagement gehören zum Kerngeschäft der IT-Abteilung. Nutzt nun ein Arbeitnehmer oder eine Fachabteilung Freeware, die für den privaten Gebrauch kostenlos, für die berufliche Nutzung aber durchaus lizenzpflichtig ist, kann ganz schnell eine Unterlizenzierung entstehen, die gegen das Urheberrechtsgesetz verstößt. Das kann nicht nur Schadensersatzansprüche nach sich ziehen, sondern auch eine strafrechtliche Verfolgung. Natürlich kann man jetzt einwenden, dass doch auch der Arbeitnehmer haftet, weil er zur Wahrung der Interessen des Arbeitgebers und des Betriebs verpflichtet ist. Hier gibt es allerdings diverse Haftungsbeschränkungen zugunsten des Arbeitnehmers. Unternehmen sollten also nicht darauf hoffen, im Ernstfall den Mitarbeiter belangen zu können, wenn der nicht nachweislich grob fahrlässig oder vorsätzlich gehandelt hat.



4. Vorbeugen durch Aufklärung

Um Schatten-IT in den Griff zu bekommen, muss sich die IT-Abteilung in Zusammenarbeit mit den Fachabteilungen zielgerichtet damit auseinandersetzen, wie sie Mitarbeiter für das Thema Datensicherheit und Compliance-Anforderungen sensibilisieren und ihnen gleichzeitig eine nutzerfreundliche Umgebung bieten können. Beispielsweise könnten Mitarbeiter dazu ermutigt werden, selbst Verbesserungsvorschläge für IT-Anwendungen einzubringen. Diese gehören anhand der Richtlinien und Anforderungen des Unternehmens bewertet und sollten – sofern sie diesen entsprechen – Eingang in die Softwareausstattung finden.

Ein generelles Nutzungsverbot von Software außerhalb des Beschaffungsprozesses oder eine autoritär agierende IT-Abteilung sind hingegen nicht zweckmäßig. Die IT muss Alternativen bieten. Oft ist es das Nicht-Wissen über die möglichen Konsequenzen der Nutzung bestimmter Soft- und Hardware, die Arbeitnehmer dazu bewegt, Lösungen an der IT vorbei zu nutzen. Natürlich bieten sich auch Richtlinien an für den Umgang mit IT, die oft als Anhang zum Arbeitsvertrag unterschrieben werden müssen und damit auch rechtliche Relevanz besitzen.

Am Konstanzer Institut für Prozesssteuerung entstand beispielsweise eine Entscheidungsmatrix für die interne IT-Abteilung, mit der Schatten-IT auf einer Skala von niedrig bis hoch nach Qualität auf der einen sowie Relevanz und Kritikalität auf der anderen Seite bewertet wird. Darauf basierend, ist es dann relativ einfach, Prozesse in ‚registrieren‘, ‚koordinieren‘ und ‚renovieren‘ zu unterteilen. Danach wird beurteilt, welche Software weiterbetrieben werden darf (da wichtig & unkritisch), aber registriert werden muss, welche modifiziert (da sicherheitskritisch) oder wo deren Nutzung renoviert (da unwichtig & kritisch), sprich untersagt und durch ein anderes System ersetzt werden muss.

VORBEUGEN

Ein grundlegendes Anpassen zu einem Selbstverständnis als Dienstleister würde jedoch jeder IT-Abteilung gut tun. Die Mitarbeiter für sich gewinnen heißt erst einmal ein Verständnis für sie zu entwickeln. Und dies kann nur durch eine gepflegte und offene Kommunikation erreicht werden. Insbesondere der Umgang mit den „Digital Natives“ sollte als Chance begriffen werden.

Sie haben durch ihr grundsätzlich besseres Technikverständnis eine hohe Affinität zum Thema. Rigide durchgreifende Administratoren sind also fehl am Platz. Vielmehr sollten innovative Ansätze und Initiativen seitens der Mitarbeiter Eingang in den Beschaffungsprozess finden.

Kenne Deinen **FEIND!**





Folgende Ratschläge an alle Unternehmen sollten Berücksichtigung finden:

1. Kenne Deinen Feind – Identifizieren Sie mögliche Ursachen in den Fachabteilungen
2. Nutzen Sie diese Erkenntnisse für einen Dialog zwischen IT und Fachabteilungen, der auf einen sinnvollen Kompromiss zwischen Sicherheit und Produktivität abzielt
3. Sensibilisieren Sie Ihre Mitarbeiter in Punkto Datensicherheit
4. Bieten Sie ihnen Alternativen an, die gleichzeitig Produktivität erhöhen und größtmögliche Sicherheit liefern
5. Identifizieren Sie Lösungen, die Schatten-IT obsolet machen. Nutzen Sie beispielsweise mehrfach verschlüsselte Filesharing Systeme.

VORBEUGEN



5. Alternative Lösungen

In manchen Szenarien ist Schatten-IT trotz aller Bemühungen nicht vollständig zu beseitigen. So können unter Umständen die angebotenen richtlinienkonformen Ersatzlösungen bezüglich Effizienz nicht mit den gewohnten Werkzeugen mithalten, oder die Modernisierung ist schlicht zu umfassend oder teuer. In Solchen Fällen sollte ein Umdenken bei der IT und den Verantwortlichen einsetzen. Die Überlegung sollte hier weg von einem restriktiven „Wie kann ich das verhindern, dass alle tun, was sie wollen?“ und hin zu einem positiven „Wie kann ich maximale Sicherheit gewährleisten, während alle tun, was sie wollen?“ gehen.

Die große Gefahr von Schatten-IT ist, wie oben beschrieben, dass die Daten unkontrolliert und potentiell ungeschützt erstellt und bewegt werden. Dadurch entstehen neben den rechtlichen natürlich auch ganz unmittelbare Konsequenzen für den Geschäftserfolg selbst. Wird ein Zwischenfall durch Datenverlust oder -diebstahl bekannt, drohen Reputationsverlust, Ausfälle in der Business Continuity und damit direkte Profitabilitätsverluste. Datensicherheit ist mittlerweile also integraler Bestandteil der Unternehmensstrategie.

Die konstante Absicherung aller Daten – auf allen Servern, im Datenzentrum und auf allen Endgeräten – durch Backups in hoher Frequenz ist hier oberste Priorität. Zudem wird durch umfassende Lösungen von Anbietern wie Code42 über die Backup-Funktionen an allen Endpunkten ständig Transparenz über den Verbleib der Daten sichergestellt.

Die Kombination aus automatischem Backup, schnellem Recovery und lückenloser Sichtbarkeit bildet eine Art abgesicherten Kontext, sollte Schatten-IT verwendet werden. Es kann von der IT nachverfolgt werden, wann welche Daten an welchem Ort sind und so existieren keine blinden Flecken oder abgeschottete Silos mehr. Im Verlustfall werden die geschäftskritischen Daten innerhalb von Minuten wiederhergestellt, sodass die Business Continuity zu jeder Zeit gewahrt bleibt. Bei Attacken oder Diebstahl kann genau nachverfolgt werden, wann und wo der Zwischenfall passiert ist und entsprechende Sicherheitsmaßnahmen können implementiert werden.

6. Fazit

Schatten-IT ist ein brandaktuelles Thema – unbestritten. Aber es ist kein Thema, dem ein Unternehmen nicht Herr werden kann. Und zwar aus technisch-funktionaler Sicht aber auch aus organisatorischer Sicht. Zum einen gibt es Stand heute Lösungen, die ein sicheres Filesharing über die Cloud ermöglichen. Zum anderen kann mittels einer erhöhten Sensibilisierung intern



**BE
PREPARED!**

ein stärkeres Bewusstsein für das Thema geschaffen werden. Schatten-IT birgt nämlich auch viele Chancen in sich. Neben einem Umdenken was Sensibilisierung der Belegschaft und Modernisierung der IT-Landschaft kann somit auch der proaktive Antrieb der Fachabteilungen, alternative Lösungen nutzen zu wollen als tatsächliches Commitment zum Unternehmen verstanden werden. Und dies gilt es freilich zu fördern!

FAZIT



7. Haftungsfragen und Lösungsansätze mit Hinblick auf die EU-DSGVO

Der Begriff Schatten-IT steht für IT-Anwendungen, die in Organisationen genutzt werden, ohne in die eigentliche IT-Landschaft eingebettet zu sein – sprich es werden Systeme und/oder Software durch Abteilungen oder einzelne Mitarbeiter parallel zur offiziellen IT-Infrastruktur genutzt. In der Regel ist diese Nutzung auch nicht von der IT-Abteilung genehmigt worden.

Für die unternehmensinternen IT-Abteilungen ist dieser unkontrollierte Wildwuchs natürlich ein Alptraum – wenn unbemerkt Hard- und Software genutzt wird, die nicht den gleichen Sicherheitsrichtlinien unterliegen, wie die offiziell im Unternehmen eingesetzten Technologien.

Laut der aktuellen CTRL-Z-Studie von Code42 darf das Risiko von Schatten-IT nicht unterschätzt werden. Drei Viertel (75 Prozent) der befragten CEOs und über die Hälfte (52 Prozent) der betrieblichen Entscheidungsträger gaben zu, Anwendungen oder Programme zu verwenden, die von ihrer IT-Abteilung nicht freigegeben wurden. Und das, obwohl 91 Prozent bzw. 83 Prozent glauben, dass ihr Verhalten ein Sicherheitsrisiko für das Unternehmen darstellen könnte.

Der durchweg gut gemeinte Wunsch nach mehr Effizienz ist hier Vater des Verhaltens. Das ändert jedoch nichts an den Risiken für die Datensicherheit – gerade im Hinblick auf die kommende Datenschutzgrundverordnung (DSGVO). Daher ist es wichtig, auch in diesem Kontext einen genauen Blick auf die Gefahren, Haftungsfragen und Lösungsansätze für Schatten-IT zu werfen.

Von
RA Robert Niedermeier
CIPP/E CIPT CIPM FIP
und
Luisa Domenichini
LL.M. (UC Berkeley)



APPENDIX



1. Gefährdungspotential in der Praxis

Schatten-IT scheint insbesondere im Kontext Cloud-Computing weit verbreitet. Das belegt der "Cloud Adoption & Risk Report Q1 2015" von Skyhigh Networks. Demzufolge kommen in Unternehmen durchschnittlich 738 Cloud-Dienste zum Einsatz, aber nur weniger als ein Zehntel davon sind bei der IT-Abteilung bekannt und genehmigt. 82 Prozent der befragten Mitarbeiter gaben gegenüber Skyhigh zu, inoffizielle Cloud-Apps zu nutzen. Als Hauptgründe nannten sie die Vertrautheit mit den betreffenden Anwendungen aus dem Privatgebrauch sowie langwierige Genehmigungsverfahren in der jeweiligen IT-Abteilung. Somit werden auch sämtliche Service Level Agreements umgangen, die durch die IT-Abteilung gewährleistet werden – ein effizienter und zuverlässiger IT-Support scheint damit gefährdet. Auch in den Marketingabteilungen ist Schatten-IT ein großes Thema: Laut der Umfrage „IT Security in the Age of the Cloud“ von CSA und Skyhigh Networks gibt ein Großteil der Befragten IT-Spezialisten (31,9 Prozent) an, dass die Marketingabteilung am häufigsten nicht genehmigte Anwendungen einsetzt.

Sie stehen unter Druck mit eingeschränkteren Budgets immer noch mehr Leads für den Vertrieb zu generieren. Die Marketingabteilungen tun vermeintlich nichts „Böses“, sondern handeln im Sinne der Effizienz sozusagen im guten Glauben. Seien es Analyse-Tools, Werkzeuge zur Marketing-Automation oder ganz banale Filesharing Tools. Die Nutzung ist nur ein paar Mausklicks und eine Kreditkartennummer entfernt. Und die IT-Abteilungen können dieser Entwicklung kaum noch standhalten. Sie haben zumeist gar keine Ahnung davon, was in der Marketingabteilung vor sich geht. Und dem Marketeer wäre es ohnehin ein echtes Rätsel, warum er darüber, dass er seinen Job richtig und gut mache, auch noch die IT informieren sollte?

APPENDIX



2. Datenschutz und Datensicherheit: Haftung

Vor allem im Hinblick auf das Thema Datenschutz und Datensicherheit stellt Schatten-IT eine große Gefahr dar. Das gilt spätestens dann, wenn der Vertriebsmitarbeiter eines Cloud Services anruft und mitteilt, dass mehrere hundert Mitarbeiter unter der Unternehmens-Emailadresse „privat“ oder zumindest unkontrolliert den Speicherdienst nutzen und man doch über eine Unternehmenslizenz nachdenken möge.

Bleibt man bei dem Beispiel Datenübertragung durch Cloud Services, muss der CIO beachten, dass hier nach Art. 24 ff. EU-DSGVO eine Auftragsverarbeitung vorliegen könnte. Der unbemerkt benutzte Cloud-Service-Anbieter wäre damit als verlängerter Arm des Unternehmens tätig und gem. Art. 28 EU-DSGVO sogenannter Auftragsverarbeiter. Dennoch bleibt das Unternehmen nach Art. 24 EU-DSGVO die verantwortliche Stelle für die Daten.

In einer solchen Konstellation fehlt es dann in der Praxis an einer erforderlichen vertraglichen Vereinbarung zum Datenschutz zwischen dem Unternehmen und dem Cloud Dienstleister. Gehen auf diesem Wege etwa personenbezogene Mitarbeiter- und/oder Kundendaten verloren, kann das zukünftig gem. Art. 83 IV a EU-DSGVO ein Bußgeld von bis zu 10 Mio. Euro für das betroffene Unternehmen bedeuten.

APPENDIX



3. Datenschutz und Datensicherheit: Lösungsansätze

In diesem Kontext ist festzustellen, dass sich Mitarbeiter meistens nicht über die Konsequenzen ihrer Taten bewusst sind. Um ungewollte Rechtsverstöße und Haftung zu vermeiden, ist es deshalb äußerst wichtig das Bewusstsein zum Thema Schatten-IT zu steigern.

3.1 Awareness

Mitarbeiter sollten regelmäßig geschult werden und es sollten Verhaltensregeln beispielsweise im Umgang mit personenbezogenen Daten implementiert werden. Die Mitarbeiter sollten darüber hinaus dazu angehalten werden bei ersten Anzeichen oder Vermutungen von EDV-Problemen oder von fremder Soft- oder Hardware diese den zuständigen IT-Administratoren zu melden oder sich vertrauensvoll mit dem zuständigen Datenschutzbeauftragten in Verbindung zu setzen.

3.2 Vertraulichkeit und Verschlüsselung

Es sollte sichergestellt werden, dass persönliche Daten nur an vertrauenswürdige und bekannte Empfänger weitergegeben werden, sofern für den Datentransfer das Internet genutzt wird, sollten Anonymisierungsverfahren eingesetzt werden. Temporäre Dateien sollten soweit möglich regelmäßig gelöscht werden, wobei bei Datenlöschung immer auf eine komplette Löschung zu achten ist, um eine Wiederherstellung der entsprechenden Daten zu verhindern. Bei dem Versand von Dokumenten als E-Mail-Anhang sollten geheime Inhalte entfernt werden oder die Dokumente hinreichend verschlüsselt werden.

Ein zuverlässiges Datensicherungskonzept ist unverzichtbar, weil beispielsweise Festplatten-defekte oftmals zu einem vollständigen Datenverlust führen oder aber die Datenwiederherstellung extrem aufwendig ist und personelle Ressourcen bindet oder erhebliche Kosten für externe Dienstleister verursacht. So ist es zwingend notwendig, dass sich der jeweilige Nutzer sowohl gegenüber seinem Endgerät als auch dem Netz der Institution erfolgreich authentifiziert, dass Daten auf den Endgeräten verschlüsselt werden und eine regelmäßige Sicherung der (mobilen) Daten im Netz der Institution erfolgt, um einen größtmöglichen Schutz vor Verlust und gegen Vertraulichkeitsverletzungen sicherzustellen. Bei der Sicherung sollte darauf geachtet werden, dass auch regelmäßig Endgeräte-Backups aller Laptops und Desktops erfolgen, nicht nur der Server und Datenzentren, um stets Transparenz über den Verbleib der Daten zu erhalten. Zum Einsatz kommen hier auch kryptographie-gesicherte VPN (Virtual Private Network), um die jeweilige Kommunikationsverbindung zwischen Endgerät und Netz der Institution vor unbefugtem Zugriff Dritter zu schützen.

3.3 Organisatorische Anweisungen

Zwingend notwendig erscheint in diesem Zusammenhang auch die Aufstellung von Anwenderrichtlinien, in denen die Nutzer auf ihre Sorgfaltspflichten hingewiesen werden, um weitestgehend Risiken durch Nachlässigkeit zu reduzieren.

Sicherheitspasswörter und deren Gültigkeitsdauer, Sicherheitsstufe und Aufbewahrung sind verbindlich festzulegen, automatisch gespeicherte Passwörter bei Online-Formularen sind zu verhindern. Programme, die in ständiger Verbindung mit einem Server stehen, sollten soweit möglich deaktiviert werden.

Freigaben für Netzwerkverbindungen sollten regelmäßig auf ihre Notwendigkeit und Aktualität überprüft werden und gegebenenfalls rückgängig gemacht werden. Kabellose Internetverbindungen sollten verschlüsselt aufgebaut werden.

Externe Datenspeichergeräte, wie beispielsweise persönliche USB-Sticks usw. sollten verboten werden.

Sorgen Sie für
SICHERHEIT





**ALWAYS IN
SECURE**

Nachfolgend ein Überblick exemplarischer Lösungsansätze zur Vermeidung von Schatten-IT und für die EU-DSGVO-konforme Cloud-Nutzung:

1. Information und Dokumentation zu Datensicherheit nach Innen und Außen

- ☐ Web-Based Trainings
- ☐ Schulung neuer Mitarbeiter bei Arbeitsantritt zum Datenschutz
- ☐ Vendor Risk Scanning von Anbietern und deren Subunternehmer

2. Neuverhandlungen über die Datenverarbeitung mit Cloud Anbietern

- ☐ Klassifizierung von Sektoren und Übertragungswegen
- ☐ Einsatz zusätzlicher Datensicherheit für vulnerable Sektoren und Datentransfer

3. EU-DSGVO Awareness

- ☐ Flyer zu EU-DSGVO an alle Mitarbeiter
- ☐ Unterbindung der unkontrollierten Nutzung von Speicherdiensten

4. Cyber-Security Maßnahmen erhöhen

- ☐ Automatische Erfassung und Auswertung von Log-Daten an neuralgischen Stellen
- ☐ Einsatz von VPN Clients
- ☐ regelmäßige und umfassende Sicherung aller Daten durch Server-, Datenzentrum- und Endgeräte-Backup

APPENDIX



SICHERHEIT ZAHLT SICH AUS!

5. Schaffung personeller Datenschutzstrukturen

- ☐ Ernennung eines Datenschutzbeauftragten
- ☐ Benennung eines dedizierten Datenschutzansprechpartners

6. Datenverschlüsselung in der Cloud

- ☐ Authentifizierung an allen Geräten
- ☐ End-to-End Verschlüsselung bei sensiblen Datenkategorien

7. Überwachung und Kontrolle über die Standorte der Daten

- ☐ Erfassung aller Dataflows (Data Mapping)
- ☐ Klassifizierung der Datenkategorien in einer Heatmap
- ☐ Datensicherung in hoher Frequenz zur Sicherstellung der Transparenz über den Verbleib der Daten

Die Autoren:

RA Robert Niedermeier
CIPT CIPM CIPP/E FIP ist seit 27 Jahren als externer Datenschutzbeauftragter in ganz Europa tätig (www.cyberlegal.eu).

Luisa Domenichini
ist juristische Beraterin im Datenschutz. Sie besitzt einen LL.M. von der Universität Berkeley und hat ihr erstes juristisches Staatsexamen in Deutschland absolviert.

APPENDIX



Das Phänomen Schatten-IT

Wenn gute Absichten plötzlich zum Problem werden

