EUROPEAN EXPERT GROUP FOR IT-SECURITY

eicar

Schatten-IT:

Fallstrick der digitalen Transformation

In Zusammenarbeit mit:

WICK HILL

Inhalt

VORWORT

Vorwort von Rainer Fahs
Chairman der EICAR

Sehr geehrte Damen und Herren,
derzeit schwebt neben den bekannten Bedrohungsszenarien, mit denen IT-Abteilungen konfrontiert sind, ein weiteres nebulöses Thema durch die Hallen vieler Unternehmen: Schatten-IT. Der Begriff täuscht jedoch ein wenig. Es geht hier primär nicht um eine Bedrohung auf technischer Ebene, sondern das Problem ist vielmehr organisatorisch begründet. Ferner scheint die Motivation für das Phänomen auch nicht dem Grundsatz eines klassischen Bedrohungsmusters zu entspringen. Es geht also nicht unbedingt in erster Linie darum, dass ein Angreifer Malware einsetzt, um einen Schaden anzurichten oder eine Website mit DDoS-Attacken kolpotiert. Schatten-IT ist vielmehr eine Konsequenz aus der gesellschaftlichen Veränderung. Die digitale Transformation und ein sich verändernderes Verhalten im Umgang mit Informationen sind ursächlich für das Thema. Dennoch ist Schatten-IT ein nicht zu unterschätzendes Risiko für Unternehmen. In dem Moment, in dem 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.

Liebe Grüße,
Rainer Fahs

Vorwort von Helge Scherff
Geschäftsführer Wick Hill GmbH

Liebe Leser(innen),
das Ihnen vorliegende Positionspapier über Schatten-IT liegt uns sehr am Herzen. Denn wir unterstützen die Aufklärung und die Sensibilisierung zu aktuellen Themen rund um die IT-Sicherheit. Als Value Added Distributor verstehen wir uns in der Rolle eines Vordenkers, der Bewußtsein schafft. IT-Sicherheit kann nämlich nicht nur auf der technischen Ebene erfolgen. Erst über einen entsprechend sensiblen Umgang mit Informationstechnologie kann ein umfassender Schutz der EDV geschaffen werden. Daher sehen wir uns in der Pflicht, Aufklärungsarbeit zu leisten.
Schatten-IT ist ein interessantes Phänomen. Es ist ein Beispiel dafür, wie aus einem organisatorischen Bedarf ein Sicherheitsproblem für eine ganze Organisationsstruktur entstehen kann. Auf den ersten Blick scheinbar wenig problematisch, entpuppt sich Schatten-IT als eine recht komplexe Gefahr. Anhand von Schatten-IT wird deutlich wie sehr organisatorische und technische Sicherheit Hand in Hand funktionieren müssen. Deshalb gibt es in Unternehmen Regelwerke, die den genauen Umgang mit Informationstechnologie beschreiben. Schatten-IT verdeutlicht warum dies so sinnvoll ist.

Herzlichst Ihr,
Helge Scherff

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 verwendet. In der Regel wird diese Nutzung auch nicht von der IT-Abteilung genehmigt.

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

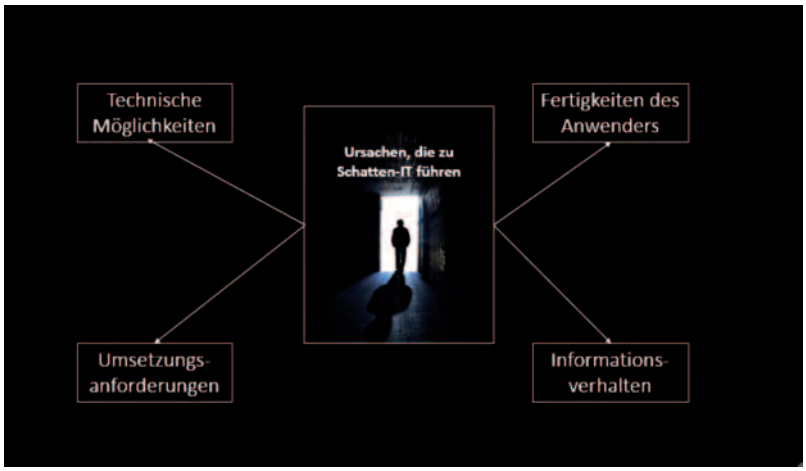
Ein moderner Mitarbeiter der Generation Y mag jetzt vielleicht denken, das dürfte doch heutzutage kein Problem mehr darstellen. Da geht Usability, Produktivität und Funktionalität doch eindeutig vor. Außerdem, so ein vielgehörter Satz, sei doch die interne IT viel zu unflexibel, um die Bedürfnisse der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

Doch gibt es noch einen weiteren Widerspruch, der auch die abteilungsübergreifende Kommunikation deutlich erschwert: Aus organisatorischer Sicht und insbesondere aus Gründen der Unternehmenspolicy 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?

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 zur Commodity geworden. Nehmen wir einmal beispielhaft Marketingabteilungen. Sie ste-

hen 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. Ganz im Gegenteil! Das Zeitalter der digitalen Transformation steht im Zeichen der Marketing Automatisierung – es soll ja schließlich Zeit und Geld sparen.

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 gibt. 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. 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 Marketer wäre es ohnehin ein echtes Rätsel, warum er darüber, dass er seinen Job richtig und gut mache, auch noch die IT informieren solle?

Langer Rede, kurzer Sinn – die technischen Möglichkeiten im Informationsumgang haben derzeit einen Stand erreicht, bei dem es zur echten Herausforderung wird, dem Tempo noch mit 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 die Datenvolumina vor Augen führt, die Server inzwischen zu verarbeiten im Stande sind, wird dies sehr deutlich: Hat man vor nicht allzu langer zeit noch Festplatten mit 5 Gigabyte beim Elektrofachhandel kaufen können, bewegen wir uns inzwischen in der Größenordnung von Terabyte. Und wenn der Anwender erst einmal in den Genuss dieser technischen Möglichkeiten gekommen ist, will er darauf logischerweise nicht mehr verzichten, weder im privaten Umfeld, noch im beruflichen.

Ein Beispiel: 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 ge-

schossen und ausgewählt – nun müssen nur noch die einzelnen Elemente zusammengefügt werden. Die Übermittlung der Texte ist recht einfach, da diese oftmals 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 störungsanfällig und noch dazu 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.

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 einzuschleusen, ist gefährlich leicht.

Die Nutzung von Filesharing-Diensten bietet noch ein weiteres Gefahrenszenario. Der Sender übermittelt seine Daten zunächst verschlüsselt an den Dienstleister. 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 in wie weit die Vorwurfsvermutung gilt, sofern sich eine Abteilung Werkzeugen aus dem Netz bedient, die entsprechende Arbeitserleichterungen nach sich ziehen.

Eine weitere Ursache für das Phänomen ist dabei sehr interessant: die Generation Y oder auch Millenials genannt. Sie bilden mittlerweile eine wichtige Berufsgruppe. Diese „digitalen natives" sind mit dem Internet, sozialen Medien und mobilen Endgeräten groß geworden. Nicht nur aus der Macht der Gewohnheit übertragen sie nun die Verhaltensmuster ins Berufsleben. Für diese Generation gehört der Umgang mit digitalen Informationen zum Lifestyle. Sie postulieren in Unternehmen eine „always on" Attitude und sind daher auch nicht in klassische Unternehmenspolicies hinein zu zwängen. Und da die Millenials 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 wichtiger 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 Millenials oft individuelle Arbeitsmethoden entwickeln, die den Einsatz von alternativen Arbeitsmitteln und Anwendungen einschließen. Hier wäre es sich mit Sicherheit ratsam, 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 vieldiskutierte 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. Heute schon sind Kernkraftwerke und Telekommunikationsanbieter dazu verpflichtet IT-Sicherheitsvorfälle zu melden. Setzen die Unternehmen dies nicht um, drohen empfindliche Bußgelder.

Damit fügt sich dem Reigen von Compliance-Anforderungen an deutsche Unternehmen eine weitere Komponente hinzu. Die Regelungsdichte nimmt dadurch immer weiter zu. Darüber hinaus beschäftigt sich die deutsche Rechtsprechung zunehmend mit Fragen der Haftung von Management und Aufsichtsorganen. Hier immer sämtliche Fallstricke im Blick 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. Dadurch können Sicherheitslücken 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 Anbieter, wenn die Daten nicht zusätzlich verschlüsselt werden. Gehen hier Daten verloren, 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 haftet die Geschäftsführung, der Finanzvorstand, der CIO oder der Compliance-Verantwortliche unter Umständen sogar persönlich für Vorfälle. Der Bundesgerichtshof 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 kön-

nen.“ 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? 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: 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 gehört 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, entsteht eine Unterlizenzierung, die gegen das Urheberrechtsgesetz verstößt. Das kann nicht nur Schadens- ersatzansprüche 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 fährlässig 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 auseinander setzen, 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 sollten anhand der Richtlinien und Anforderungen des Unternehmens bewertet werden und – 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 zweckdienlich. Die IT muss Alternativen bieten. Oft ist es das Unwissen 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 für den Umgang mit IT an, 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 untersagt und durch ein anderes System ersetzt werden muss, da sie unwichtig und zudem kritisch ist.

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. Dies kann nur durch eine gepflegte und offene Kommunikation erreicht werden. Insbesondere der Umgang mit den „digitalen 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.

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 die Produktivität erhöhen und größtmögliche Sicherheit liefern.

5. Identifizieren Sie Lösungen, die Schatten-IT obsolet machen. Nutzen Sie beispielsweise mehrfach verschlüsselte Filesharing Systeme, die keine Backdoor-Möglichkeiten bieten (keine US-amerikanischen Hersteller).

5. Alternative Lösungen

In einem ähnlichen Tempo, wie sich die Cloudlösungen entwickeln, haben sich mittlerweile auch Alternativlösungen entwickelt. Aber nur wenige bieten die integrierte Sicherheitsfunktionalität, die den Unternehmensvorschriften genügt. Ein sinnvolles Beispiel gibt die Zusammenarbeit zwischen SSP Europe und der Deutschen Telekom. Hier hat die Deutsche Telekom die Möglichkeit eine Technologie als OEM-Lösung zu nutzen, die das Look & Feel des Telekom-Riesen in magenta ermöglicht. Somit fühlt es sich für den Mitarbeiter an, als gehöre die Lösung zur Unternehmens-IT.

Das renommierte Fachmagazin COMPUTERWOCHE beschreibt wie folgt das Projekt: „Die vom Münchener Sicherheitsspezialisten SSP Europe entwickelte Enterprise File Sync and Share Lösung (EFSS) Secure Data Space, welche die Deutsche Telekom als OEM unter dem Namen Secure Data Drive vermarktet, ist so konzipiert, dass sie von großen Unternehmen als Standard Account für den Datenaustausch der Mitarbeiter sowie in Spezialbereichen verwendet werden kann. Für Patrick Glaffig, Produktmanager bei der Deutschen Telekom, könnte der Zeitpunkt nicht besser gewählt sein: ‚Unternehmen denken durch die zahlreichen Vorfälle und Diskussionen rund um das Thema Datenspionage und das Risiko privater Accounts um. Daher ist es uns besonders wichtig, unseren Kunden die höchstmögliche Sicherheit aus und in Deutschland für ihre Daten zu bieten.‘ Die Triple-CryptTM Technology sichert Daten gleich dreifach: direkt am Endgerät des Benutzers, während der Datenübertragung und im Cloud Speicher selbst. Ergänzt wird die umfangreiche Sicherheitsarchitektur durch die Rechenzentren der Telekom in Deutschland, welche nach der ISO/IEC-Norm 27001 zertifiziert sind und ein umfassendes Informationssicherheits-Managementsystem gewährleisten. Damit wird Secure Data Drive auch gegen den Zugriff außereuropäischer Staaten geschützt.

Der Secure Data Drive wird von der Telekom als Cloud Service oder On-Premise-Lösung angeboten, wobei Daten entweder direkt in der Cloud des Providers gespeichert werden oder bei der On-Premise-Lösung innerhalb des Unternehmens. Letzteres ist besonders für Unternehmen mit strengen Sicherheits- und Compliance-Vorgaben geeignet. Die flexiblen und skalierbaren Lizenzregelungen können an die aktuellen Anforderungen im Unternehmen angepasst werden.“

Es gibt also bereits heute Lösungen, die das Thema Schatten-IT quasie „ersetzen“. Das scheint ein richtiger Weg zur Bewältigung der Herausforderungen zu sein.

6. Fazit

Schatten-IT ist ein heikles Thema – unbestritten. Aber es ist kein Thema, das ein Unternehmen nicht in den Griff bekommen kann. Und zwar aus technisch-funktionaler, aber auch aus organisatorischer Sicht. Zum einen gibt es zum jetzigen Zeitpunkt Lösungen, die ein sicheres Filesharing über die Cloud ermöglichen. Zum anderen kann mittels einer erhöhten Sensibilisierung intern ein stärkeres Bewußtsein für das Thema geschaffen werden. Schatten-IT bringt allerdings auch viele Chancen mit sich. Neben einem Umdenken und Sensibilisierung der Belegschaft sowie 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!

EUROPEAN EXPERT GROUP FOR IT-SECURITY

eicar

EICAR Office
Obergasse 28A, 86943 Thaining
Germany

Tel: +49 (0)8194 / 99 84 99
Fax: +49 (0)8194 / 99 85 01

office@eicar.org
www.eicar.org