The IT Manager Who Shattered Shadow IT (Die Schattenseiten der Schatten-IT)

Bieten Sie Schatten-IT die Stirn und übernehmen Sie wieder die Kontrolle über Ihren Software-Stack

Der Begriff „Schatten-IT“ ist in Unternehmen heutzutage in aller Munde. Vielen Organisationen ist jedoch nicht klar, wie viele Risiken mit der nicht genehmigten Installation technischer Lösungen auf eigene Faust verbunden sind. Einer Studie zufolge nutzen große Unternehmen im Schnitt etwa 1220 verschiedene Cloud-Services. Das sind 13 Mal so viele wie die 91 Services, die den IT-Abteilungen bekannt sind. Schatten-IT läuft nicht nur der Arbeit von IT-Abteilungen direkt zuwider, sondern kann auch Sicherheitslücken und unnötige Kosten verursachen. In der Regel nutzen Mitarbeiter Schatten-IT, weil sie glauben, dass es ihrem Unternehmen und dessen IT-Abteilung Zeit und Geld spart. In Wirklichkeit führt die Nichteinbindung der IT dazu, dass die unverzichtbaren Leistungen, die sie bereitstellt – Management, Integration, Sicherheit und Compliance-Sicherung – umgangen werden und nicht richtig greifen können.

Stellen Sie sich einmal eine Welt vor, in der Schatten-IT das gesamte Unternehmen bis in den letzten Winkel durchdrungen hat und eine größere Bedrohung für dessen Sicherheit, Wirtschaftlichkeit und Effizienz darstellt, als man sich das jemals hätte träumen lassen. Das ist eine Art Wilder Westen: Schießereien auf der Straße, junge Damen in Not und im Hintergrund das Geklimper eines alten Saloon-Klaviers. Da treten Clark, der IT-Manager (und der Held dieser Geschichte), seine Chefin Cynthia, der CIO, und sein treuer Begleiter Steve, der Systemadministrator, auf den Plan. Die drei sitzen schweigend nebeneinander. Ihre Abteilung hat die Kontrolle verloren und niemand weiß so recht, welche Technologie wo im Unternehmen eingesetzt wird. Die Konsumerisierung der IT bzw. der Zyklus, in dem Mitarbeiter bei Verbrauchern beliebte Technik im Büro einführen, hat es ihnen einfach gemacht, technische Lösungen zu nutzen, von denen die IT-Abteilung nichts weiß.

Dieses Problem betrifft nicht nur Clark und sein Team. In einer Umfrage von Intel zum Thema Sicherheit gaben 23 % der Befragten an, dass ihre Unternehmen sich ohne Hilfe der IT um Sicherheitsbelange kümmern.

Eines Tages hatte Clark genug. Er hatte die Nase voll davon, sich ständig mit Schatten-IT herumschlagen zu müssen und nicht zu wissen, welche Technik wo im Einsatz war, um den Unternehmensbetrieb am Laufen zu halten. Also beschloss er, etwas dagegen zu unternehmen. Er rief sein Team zusammen, entwarf einen Schlachtplan und nahm mit voller Kraft den Kampf gegen die Schatten-IT auf.

Da unser Unternehmen in hohem Maße von der Genehmigung durch die IT-Abteilung abhängig ist, wollten wir mehr darüber erfahren, was Clark über alleinstehende, nicht genehmigte Anwendungen denkt. Wir wollten seine systematische Herangehensweise im Kampf gegen die Schatten-IT besser

verstehen und eine transparentere IT-Management-Kultur aufbauen.

Lifesize
Anbieter von Lösungen zur Kommunikation über die Cloud sowie von Software zur Zusammenarbeit

Clark
Ein heldenhafter IT-Manager für Unternehmen wie Ihres

Wie haben Sie das Problem gefunden? Wie sind Sie vorgegangen, um die schlimmsten Schwachstellen aufzuspüren?

Es begann alles mit einem Artikel, den ich gelesen habe. Darin stand, dass „**sieben von zehn Führungskräften nicht wissen, wie viele Schatten-IT-Anwendungen in ihrem Unternehmen verwendet werden**”. Das machte mich neugierig und ich wollte herausfinden, ob das auch auf mein Unternehmen zutraf. Mein Team hörte häufig von all diesen unterschiedlichen Anwendungen, die die verschiedenen Abteilungen nutzten, aber niemand besprach dies direkt mit uns. Manche davon waren harmlos, andere stellten möglicherweise eine Gefahrenquelle dar — und das konnten wir uns nicht leisten. Wir fingen an, engmaschig zu überwachen, ob bei unseren üblichen Scans neue, unbekannte Tools oder Anwendungen auftauchten. Dies mündete schließlich in eine unternehmensweite Untersuchung auf Schwachstellen.

Es gibt Programme, die eigens dafür konzipiert wurden, neue Anwendungen in einem Netzwerk aufzuspüren. Netzwerk-Sniffer und Sicherheitsprüfungstools können detaillierte Informationen zu neuen, unbekannten Datenströmen liefern. Durch reines Überwachen können die von Schatten-IT ausgehenden Bedrohungen natürlich nicht eliminiert werden, aber es können wertvolle Erkenntnisse gewonnen werden. Die Untersuchung, die wir durchgeführt haben, hat uns gezeigt, dass unsere Mitarbeiter Tools nutzten, von denen wir gar nichts wussten. Sie hat uns genügend Informationen geliefert, um erste Gefahreneinschätzungen vornehmen und in den schlimmsten Fällen nach alternativen Lösungen suchen zu können, die besser zu unseren Anforderungen passten.

Sind

Natürlich. Viele Mitarbeiter in

Sie auf Widerstand gestoßen, wenn Ihre IT-Organisation einige der von einer Abteilung favorisierten Tools nicht unterstützen konnte?

unserem Unternehmen arbeiten aus der Ferne, d. h. nicht im Büro. Wir haben rasch bemerkt, dass eine der damit verbundenen Herausforderungen darin besteht, dass Mitarbeiter, denen keine IT-geprüfte Möglichkeit zur Arbeit von zuhause oder von unterwegs aus zur Verfügung gestellt wird, sich selbst eine solche Möglichkeit suchen. Und das birgt natürlich Risiken, von einer unsicheren Übertragung von Dateien bis hin zum Verlust oder Diebstahl von Geräten usw. Wir haben festgestellt, dass wir durch Transparenz in Bezug auf unsere Sicherheits- und Netzwerkanforderungen unsere Mitarbeiter dazu anregen können, sich an die IT zu wenden, wenn sie auf neue Software stoßen, die sie nutzen möchten. So haben wir es geschafft, häufiger in solche Diskussionen eingebunden zu werden, und waren so in Bezug auf die Endentscheidung wesentlich besser positioniert. Sie glauben gar nicht, wie sehr sich die Leute darüber freuen, wenn man ihnen bei der Suche nach und Auswahl von Lösungen unter die Arme greift, statt alles geheim halten und alleine stemmen zu müssen.

Wie haben Sie es

Ja, zunächst schon. Schatten-IT stellt nur für Unternehmen, die sich nicht damit beschäftigen möchten, eine schwere

geschafft, dass Ihnen die Mitarbeiter Informationen zu ihrer Schatten-IT gegeben haben? Das war sicher nicht ganz einfach.

Gefahr dar — also haben wir beschlossen, uns aktiv damit zu beschäftigen. Der Trend geht dahin, dass IT-Organisationen Türen eintreten und allen, die nicht genehmigte Software nutzen, schlimmste Strafen androhen. Das finde ich etwas überzogen. Wir haben uns für eine friedvollere Herangehensweise entschieden und Abteilungen, die Schatten-IT verwendeten, einen Ausweg geboten. Statt die entsprechenden Programme direkt zu übernehmen und auszuschalten, haben wir uns das Ganze erst einmal angesehen, das jeweilige Risiko ermittelt und wo nötig den Leuten vergleichbare Lösungen angeboten, mit denen sie das gewünschte Ergebnis erzielen konnten. So konnten wir auch die mit dem jeweiligen Programm verbundenen Risiken mit ihnen besprechen. Über diese Vorgehensweise ist es uns gelungen, alle auf den gleichen Stand zu bringen sowie ein Klima des Vertrauens und der Offenheit zwischen „uns“ und „ihnen“ zu schaffen.

Wie haben Sie es geschafft, diese Strategie konsequent durchzuhalten? Das Schatten-IT-Problem, vor dem Sie standen, ist jetzt behoben. Wie aber stellen Sie sicher, dass es sich nicht wieder einen Weg zurück in Ihr Unternehmen bahnt?

Wissen Sie, das bin ich schon häufig gefragt worden, und die Antwort ist denkbar einfach. Der Schlüssel zu allem sind Beziehungen. Ich habe aktiv eine Beziehung zu jedem Abteilungsleiter aufgebaut und mich regelmäßig mit ihm oder ihr getroffen, um die Technikstrategie zu besprechen. So konnten wir einen offenen Dialog zwischen den einzelnen Abteilungen und der IT-Organisation erreichen. Enorm wichtig war auch, dass meine Chefin Cynthia, unser CIO, einen engen Kontakt zu den übrigen E-Mitarbeitern gehalten und sich mit ihnen über Technologietransparenz und die möglichen Risiken der Nutzung nicht genehmigter Technologien ausgetauscht hat.

Sie haben den Kampf gegen die Schatten-IT in Ihrem Unternehmen gewonnen. Was raten Sie IT-Abteilungen, die gerade erst damit begonnen haben, das Problem in ihrem Unternehmen anzugehen?

Man muss die Vorteile eines offenen Dialoges mit den Kollegen im gesamten Unternehmen nutzen, das sind unsere Kunden. Wir nehmen ihr Feedback auf, informieren uns über die Probleme, die sie zu lösen versuchen, und sind bereit, Auskunft hierzu zu geben. Ich wurde einmal gebeten, ein Tool zu prüfen, das bereits genehmigt worden war und von einer anderen Abteilung im Unternehmen eingesetzt wurde. In diesem Fall war es viel einfacher und günstiger, unseren Plan entsprechend anzupassen und ein paar zusätzliche Lizenzen zu erwerben, als einen ganz neuen Vertrag aufzusetzen. Der letzte Rat, den ich Ihnen geben möchte, ist, nicht die Schlagkraft einer einfach zu bedienenden Benutzeroberfläche zu unterschätzen. Achten Sie darauf, Ihre Sicherheits- und Netzwerkanforderungen mit der Benutzerfreundlichkeit der Anwendungen für den Endnutzer in Einklang zu bringen. Ich achte insbesondere darauf, eine Lösung zu finden, die sich mit unserem SSO integrieren lässt. So müssen die Mitarbeiter weniger Passwörter verwalten und aktualisieren.

Die Kombination aus unzureichender Passwortsicherheit und Schatten-IT-Anwendungen kann zu schwerwiegenden Sicherheitslücken führen. Auf unserem Blog erfahren Sie in dem Artikel „The Best Defense Against IoT DDoS Attacks“ (Die beste Verteidigung gegen DDoS-Angriffe im IoT), wie Sie Ihr Netzwerk schützen können.

Über Lifesize

Das Zusammenarbeitssystem von Lifesize wird von der IT geschätzt, da es von Anfang an auf die Schwerpunkte Sicherheit, Resilienz und Netzwerkverfügbarkeit ausgelegt wurde. Wir verfügen über mehr als zehn Jahre Erfahrung im Design von HD-Kameras und Touchscreen-Handys. Unsere intuitive Benutzeroberfläche und das gemeinsam genutzte Verzeichnis geben den Benutzern alles, was sie brauchen, um mithilfe IT-geprüfter Anwendungen effektiver zusammenarbeiten zu können. So sind keine zusätzlichen alleinstehenden Anwendungen mehr erforderlich. Die Kommunikationsströme von Lifesize unterstützen standardmäßig 128-bit AES- und TLS (Transport Layer Security)-Verschl¨¨üsselung für alle Signale. Unser Betrieb läuft zudem auf einem privaten Fasernetzwerk, über IBM Cloud. Und zu guter Letzt wird unser preisgekrönter Service durch eine finanziell abgesicherte Dienstleistungsvereinbarung (Service Level Agreement, SLA) mit rund um die Uhr verfügbarem Support ergänzt.

QUELLEN

http://blogs.cisco.com/cloud/shadow-it-rampant-pervasive-and-explosive
http://www.csoonline.com/article/3083775/security/shadow-it-mitigating-security-risks.html
http://www.digitalistmag.com/resource-optimization/2016/02/11/2016-state-of-shadow-it-04005674