nexthink

Schatten-IT: Einzelfall oder doch Alltag?

2020

Inhalt

Auf einem Blick

Schatten-IT ist ein Phänomen, das nach wie vor existiert und vielen CIOs, IT-Abteilungen und -Mitarbeitern Kopfzerbrechen bereitet. Eine Lösung dieses Konflikts kann nicht in absoluten Verboten und rigoroser Überwachung bestehen. Aufklärung für die Mitarbeiter und Dialog mit ihnen ist extrem wichtig. Der Einsatz einer Workplace Management Platform wie Nexthink kann eine große Hilfe sein, die Problematik der Schatten-IT überhaupt erst einmal zu erkennen und dann adäquat zu behandeln.

Einleitung

In der an Schlagworten sicher nicht armen IT-Welt war die „Schatten-IT“ bis vor nicht allzu langer Zeit sehr präsent: Administratoren wurde dabei unter anderem auch vorgeworfen, dass sie „ihre IT“ nicht mehr im Griff hätten. Die Nutzer würden ihnen auf der Nase herumtanzen und lieber irgendwelche Cloud-Dienste und Apps einsetzen, statt die von der IT zur Verfügung gestellten Anwendungen und Programme zu nutzen.

In der Zwischenzeit ist es wieder deutlich ruhiger um dieses Thema geworden und viele Unternehmen setzen SaaS-Dienste (Software as a Service) inzwischen standardmäßig ein oder favorisieren eine „Bring Your Own Device“-Strategie – obwohl gerade diese Lösungen von vielen Kritikern unter anderem als Initiatoren für die Verbreitung einer IT gesehen wird, die im Schatten und außerhalb der Kontrolle der IT-Mannschaft steht. Wie sieht es aktuell aus mit der IT „im Schatten“ in deutschen Unternehmen? Handelt es sich dabei um ein rein technisches Problem oder um ein grundsätzliches Missverständnis zwischen den Profis von der IT und den „normalen Nutzern“?

Die Experten des Unternehmens Nexthink haben es sich zur Aufgabe gemacht, den IT-Abteilungen und -Verantwortlichen dabei zu helfen, die Art und Weise zu verbessern und weiterzuentwickeln, wie sie Unternehmensmitarbeiter unterstützen und ihnen die benötigten IT-Dienste bereitstellen können. Dabei führen sie viele Gespräche mit Kunden und deren IT-Spezialisten und bekommen so tiefe Einblicke in die Probleme, die in diesen Beziehungen bestehen. Aktuell stellen sie in solchen Gesprächen immer wieder fest, dass das Thema „Schatten-IT“ immer noch akut ist und viele IT-Abteilungen nach wie vor tagtäglich belastet.

Dieses Whitepaper zeigt, wie Unternehmen diese Probleme und Herausforderungen angehen und beheben können. Dabei geht es nicht darum, Schuld zuzuweisen oder gar den Nutzern alles zu verbieten: Es geht darum, gute Ansätze zu erkennen, die Zusammenarbeit zu verbessern und den Anwendern endlich das Gefühl zu vermitteln, dass es „ihre IT“ ist, mit der sie an ihren digitalen Arbeitsplätzen täglich arbeiten.

Denn niemand verwendet eigene Applikationen oder SaaS-Lösungen, um seinem Unternehmen zu Schaden, sondern um seine tägliche Arbeit effizient zu erledigen, ganz im Sinne des Geschäfts. Der positiven digitalen Erfahrung der Mitarbeiter sollten IT-Organisationen nicht einfach durch Drohkulissen begegnen. Nexthink empfiehlt vielmehr, den Anwender dabei zu unterstützen, richtlinienkonform zu bleiben und im Zweifelsfall zu beraten, wie er seine Aufgaben im Einklang mit den Sicherheitsregeln des Unternehmens optimal erledigen kann.

Schatten-IT erkennen und analysieren

Nexthink erkennt effizient Applikationen und die Nutzung von Cloud-Diensten auf Endgeräten und kann das Kommunikationsverhalten analysieren und das Bedrohungspotential einschätzen. Daraus lassen sich relevante Aktionen ableiten, um die Unternehmensrichtlinien einzuhalten und Anwender vor unbewussten Aktivitäten zu schützen.

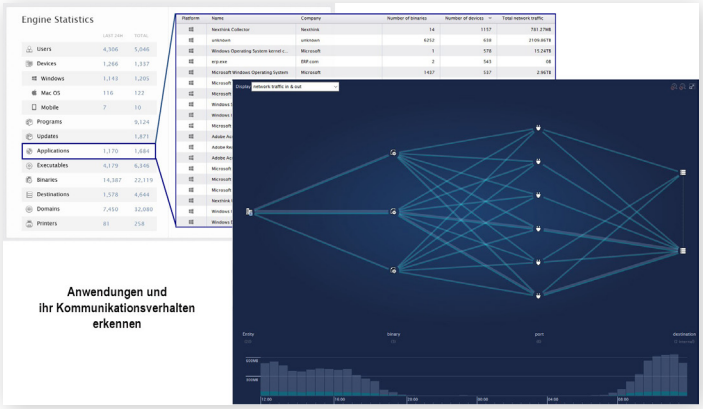

Abbildung 1 - Nexthink erkennt Applikationen, Web-Services und deren Kommunikationsverhalten

Schatten-IT: Definition und Ursachen

Auch wenn es auf den ersten Blick in einigen Unternehmen nach wie vor nicht so aussehen mag: Die Zeiten, in denen die Anwender eher unwissend und der „allmächtigen IT-Abteilung“ ausgeliefert vor ihren Computern saßen, sind schon eine ganze Weile vergangen. Das liegt aber nicht nur an den sogenannten und von der Boulevardpresse oft beschworenen „Digital Natives“, die ihre Endgeräte und Anwendungen mit in die Unternehmen und Dienststellen bringen. Es ist nicht zuletzt auch daran festzumachen, dass es fast alle Arbeitnehmer heute gewohnt sind, Dinge wie Dropbox, Cloud-Lösungen von AWS bis Azure oder Sprachassistenten auch im heimischen Umfeld wie selbstverständlich einzusetzen.

Auf diese Weise hat die sogenannte und heute oft thematisierte digitale Transformation mit ihrer Vielfalt an neuen digitalen Techniken und den damit verbundenen Möglichkeiten einen Weg in die Business-IT gefunden, der nicht immer im Sinne der CIOs, IT-Verantwortlichen und der IT-Administratoren ist: So werden dann Geräte und vor allen Dingen auch Software-Lösungen innerhalb von Firmen-Netzwerken eingesetzt und teilweise sogar darin eingebunden, die außerhalb des Einflusses der IT liegen.

Es hält Software Einzug, die von Nutzern unbemerkt von der IT eingesetzt wird, – gerade dann, wenn es um SaaS-Lösungen (Cloud-Dienste) geht, auf die Anwender aus dem Firmennetzwerk heraus einfach mit einem Browser zugreifen oder File-Sharing-Lösungen, bei denen die Daten ebenfalls unbemerkt das Netzwerk verlassen können.

Nicht zu Unrecht gibt es eine ganze Reihe von Unternehmen beispielsweise aus der Finanzbranche oder aus dem Gesundheitssektor, die den Einsatz von Cloud-Lösungen für ihre Unternehmensdaten aus Sicherheits- und/oder Compliance-Erwägungen heraus grundsätzlich verbieten. In der Praxis sind sie bei einem (immer wieder auftretenden) Umgehen dieser Verbote noch schwerer vom Phänomen der Schatten-IT betroffen. So retten sich dann viele Unternehmen und IT-Verantwortliche gerade auch im öffentlichen Bereich in eine „alles ist verboten"-Politik – mit zumeist zweifelhaftem Erfolg.

Und natürlich ist es wie im Straßenverkehr – was nutzen die besten Verbote, wenn der Mitarbeiter sie nicht versteht und sich in seiner Produktivität eingeschränkt fühlt? Und vor allem: Wenn die IT-Organisation gar nicht in der Lage ist, die Einhaltung der Verbote auch effizient zu überwachen und zu sanktionieren. Und noch dramatischer: Die IT gar nicht als Partner für das Finden optimaler Lösungen in Betracht gezogen wird.

Übersichtliche Dashboards als Steuerungselement gegen verdächtiges Verhalten

IT-Verantwortlichen fehlt oft nicht nur der Blick für Details, sondern gerade auch die Übersicht. Wie einfach wäre es doch, mit übersichtlichen Dashboards Gefahren und verdächtiges Verhalten erkennen und entsprechend reagieren zu können?

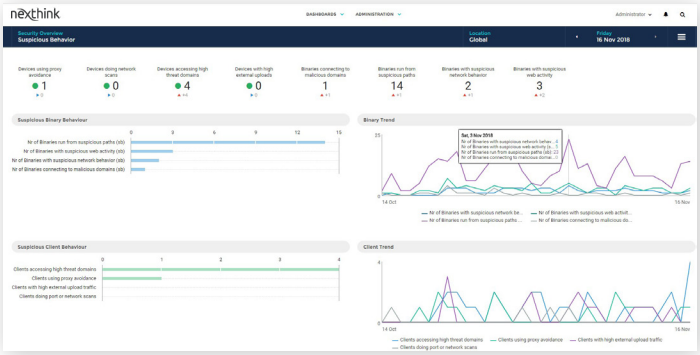

Abbildung 2 - Dashboards für bessere Übersicht

Die Sicht der IT-Profis: Es gilt ein Delta zu bewältigen

Wer sich in den Unternehmen umhört, kann häufig auf beiden Seiten – also sowohl bei den IT-Verantwortlichen und -Profis als auch bei den „normalen" Anwendern – große Unzufriedenheit feststellen – und das in Zeiten wo renommierte Analysten wie Forrester und Gartner die Bedeutung der Digitalen Erfahrung am Arbeitsplatz als einen wesentlichen Wettbewerbsfaktor ausgemacht haben. Steht doch die IT allzu oft vor der undankbaren Aufgabe, mit immer geringerem Etat und gerade in den kleineren Unternehmen auch mit einer häufig ebenso dünnen Personaldecke,

eine gut funktionierende Arbeitsumgebung für die Mitarbeiter aufzubauen und zu betreiben. Diese soll zudem noch den jeweiligen Compliance- und Sicherheits-Richtlinien des Unternehmens entsprechen. Ein Anspruch, der gerade nachdem die Europäische Union die Datenschutz-Grundverordnung im letzten Jahr „scharf geschaltet“ hat, in der täglichen IT-Welt noch viel schwieriger zu bewältigen ist und drastische finanzielle Konsequenzen nach sich ziehen kann.

Die IT-Profis haben in den Unternehmen eine Entwicklung mitmachen müssen, die zunehmend auf Zentralisierung der IT-Dienste setzt: Die meisten Anwendungen und Dienste laufen im Rechenzentrum, die Nutzer greifen dann nur noch über Remote-Terminals oder Virtual Desktops mittels einer VDI (Virtual Desktop Infrastruktur) auf die Daten und Anwendungen zu. Für die IT ist das grundsätzlich eine gute Sache, bekommt sie so doch die Endgeräte besser in den Griff und kann Compliance-Richtlinie effizienter durchsetzen und befolgen. Auf der Seite der Nutzer wird dadurch aber allzu häufig das Delta zwischen ihren Wünschen und Ansprüchen an den Arbeitsplatz und den zur Verfügung stehenden Arbeitsmitteln größer: Kennen sie doch bessere Lösungen und Dienste, die für ihre Ansprüche passender sind, als die von der IT zur Verfügung gestellten Mittel.

Im Prinzip sollten die IT-Abteilungen ja froh darüber sein, dass die Anwender Initiative und Kreativität beweisen, wenn es beispielsweise darum geht, die Daten in der Cloud zu sichern oder alternative Mail-Fächer zu nutzen, falls der firmeneigene Mail-Server „mal wieder“ nicht funktioniert. Damit die IT-Abteilungen nicht mehr als Gegner wahrgenommen werden, deren Einschränkungen man als Endnutzer nur durch Eigeninitiative und damit durch den Einsatz der zumeist auch privat präferierten Anwendungen entkommen kann – der klassische Grund für eine Schatten-IT – muss dieses Delta gemeinsam beseitigt werden. Das kann durch mehr Zusammenarbeit zwischen der IT-Abteilung und den Endnutzer gerade auch mit Hilfe entsprechender Lösungen, auf die wir hier in diesem Whitepaper noch näher eingehen, durchaus erreicht werden.

Stellen wir uns einfach einmal vor, die IT verbietet nicht einfach nur etwas, sondern schlägt eine richtlinienkonforme Lösung vor, die der Anwender noch nicht kennt? Oder - aus heutiger Sicht ebenso revolutionär – die IT tritt in die Diskussion mit dem Anwender, um zu verstehen, wie seine Anforderungen im Kontext der Unternehmensrichtlinien umgesetzt werden können?

Gedankenanstöße: Was die Nutzer wollen...

Aus der Perspektive des „normalen“ Nutzers mag gerade in der Vergangenheit oft der Eindruck entstanden sein, dass die IT-Mannschaft alles daransetzt, „ihren Anwendern“ möglichst alle Freiheiten zu nehmen. Diese in vielen Unternehmen historisch gewachsene Abneigung zwischen den IT-Fachleuten und den Anwendern sollte bei der Betrachtung der Schatten-IT keinesfalls außer Acht gelassen werden: Oftmals ist die Unzufriedenheit der Nutzer mit den ihnen zur Verfügung stehenden

Security hat massiven Einfluss auf die Anwender-Akzeptanz

Wer kennt das nicht. Morgens läuft der Antiviren-Scanner los und macht ein vernünftiges Arbeiten unmöglich, oder die Firewall blockiert schon wieder die falschen Ports. Die IT wird eher als Behinderung statt als Nutzbringer empfunden. Nexthink hilft, notwendige Schutzmaßnahmen (harte Fakten) und die digitale Erfahrung der Mitarbeiter (subjektives Empfinden) gleichzeitig zu optimieren.

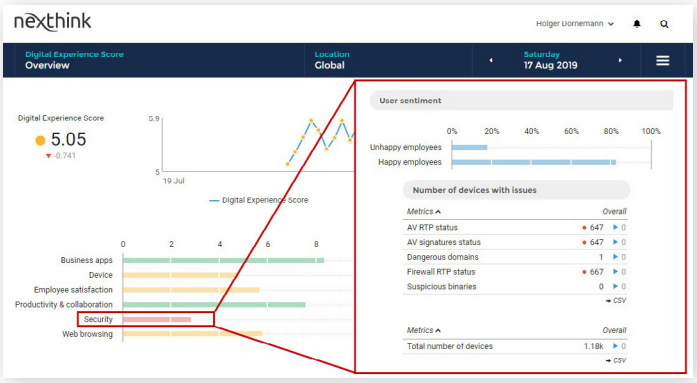

Abbildung 3 - Harte Fakten und subjektives Empfinden im Einklang

Möglichkeiten, Diensten und Programmen ein Auslöser dafür, dass beispielsweise auch ganze Fachabteilungen lieber selbst einen Dienst aus der Cloud für ihre Arbeit nutzen, als sich auf die von der IT zur Verfügung gestellten Programme zu verlassen.

Doch was wollen die Nutzer wirklich? Es ist sicher ein guter Ratschlag an die IT-Experten, einfach mal zuzuhören. In der Regel wollen Anwender ihre Arbeit möglichst gut und ohne Probleme und Hürden erledigen können. Dabei ergeht es dem Endnutzer an seinem Arbeitsplatz ähnlich wie einem Autofahrer, der nur sein Ziel erreichen will: Dabei ist es ihm in der Regel ganz gleich, ob das Gefährt via zwei oder vier Räder angetrieben wird – solange er nicht unterwegs dauernd darauf achten muss, dass auch wirklich alle vier Räder vorhanden sind. Auch die IT ist für die Nutzer kein Selbstzweck, sondern eher das „Vehikel“, um ihre Arbeit zu erledigen. Dabei mögen viele moderne IT-Systeme zwar durchaus allen Bestimmungen und Compliance-Regeln genügen, sind aber im täglichen Betrieb häufig viel zu komplex, zu schwer zu bedienen oder sie sind – warum auch immer – einfach nicht verfügbar. Wer kann es den Anwendern da verdenken, wenn sie lieber zu einfach zu bedienenden Programmen und Diensten greifen?

Soll die IT den Anwendern also alles erlauben? Die Fachleute von Nexthink konnten in Kundengesprächen immer wieder feststellen, dass es in vielen Unternehmen nach wie vor üblich ist, den Anwendern Zugriff und Nutzung selbstinstallierter Programme und Dienste zu erlauben. Solche Unternehmen können dann mit Hilfe von Nexthink leicht entdecken, was in ihrem Netzwerk genutzt wird. Das kann die IT nutzen, um mehr über „ihre Anwender“ und deren Bedürfnisse zu erfahren. Weiterhin können die IT-Fachstellen so auch feststellen, an welchen Stellen

Nachholbedarf besteht. Dabei geht es im ganz besonderen Maße darum, dass die IT mit den eigenen Nutzern im Unternehmen im Hinblick auf diese Problematik intensiv kommuniziert. Im Notfall kann die IT auch die Notbremse ziehen und vollständig verbotene Applikationen entfernen und die Kommunikation zu ungewollten Cloud-Services unterbinden.

Ganz wichtig: Hier sind Aufklärung und Dialog ganz besonders angeraten: Die IT muss den Mitarbeitern erläutern, warum sie diese bestimmte Anwendung oder diesen Dienst nicht nutzen sollten und ihnen vor allen Dingen die alternativen Möglichkeiten aufzeigen, die im Firmennetzwerk bereitstehen: Dabei kann es sich dann beispielsweise um eine sichere, zertifizierte File-Sharing-Lösung, wie etwa Microsoft OneDrive oder Google Drive, die im Unternehmen zwischenzeitlich offiziell autorisiert wurde, statt Dropbox handeln, das man nutzte, weil keine offizielle Alternative angeboten wurde. Natürlich muss für die IT-Verantwortlichen immer auch die Option bestehen, im Notfall zu intervenieren, wenn durch die Schatten-IT kritische Situationen entstehen.

Informieren statt bestrafen

Anwender, die unbewusst gegen Richtlinien verstoßen, können mit Nexthink effizient informiert, auf Alternativen hingewiesen und nach ihren Erfahrungen oder Vorschlägen gefragt werden..

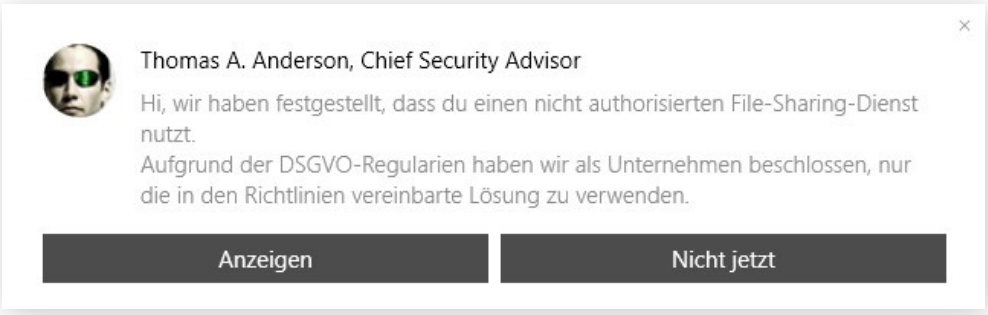

Abbildung 3 - Harte Fakten und subjektives Empfinden im Einklang

Fazit: Das Problem ist da – eine Lösung ebenfalls

Aktuell sind nach wie vor in vielen Unternehmen Lösungen und Programme im Einsatz, auf die der Begriff Schatten-IT zutrifft. Dass die Anwender immer autarker agieren (wollen) ist eine Tatsache und mit rigorosen Verbotsmaßnahmen werden Geschäftsleitung und IT dieses Problem kaum in den Griff bekommen. Auch HR Abteilungen sind daran interessiert, Mitarbeitern einen möglichst attraktiven digitalen Arbeitsplatz bieten zu können. Cloud-Lösungen und auch BYOD-Strategien sind ebenfalls Tatsachen, die nicht zuletzt dazu beigetragen haben, derartige Probleme hervorzurufen. Allerdings werden diese Techniken auch in Zukunft eine wichtige Rolle spielen – ein weiterer Grund, warum Bekämpfen beziehungsweise reines Verbieten wenig sinnvoll sind: Die Nutzer werden immer einen Weg finden.

Die Problematik wird immer mehr IT-Verantwortlichen und -Abteilungen bewusst und es setzt sich die Erkenntnis durch, dass es zunächst einmal darum gehen muss, diese Anwendungen aus dem Schatten herauszuholen und zu erkennen, wo und wie solche Programme zum Einsatz kommen. Die Experten von Nexthink sehen sich durch viele Kundengesprächen darin bestätigt, dass zwar BYOD in den deutschen Unternehmen nicht im großen Umfang zum Einsatz kommt, dass sich aber Cloud-Anwendungen, SaaS-Lösungen und lokale Apps wie Passwort-Manager u.ä. immer mehr verbreiten.

Ultima Ratio – wenn es dann gar nicht mehr anders geht

Und natürlich muss es auch eine Ultima Ratio geben, wenn von einem Arbeitsplatz erhebliches Bedrohungspotential ausgeht oder aber gut gemeine Ratschläge nicht ankommen. Dann kann Nexthink auch schon mal einen Arbeitsplatz vom Netz nehmen, Software deinstallieren oder andere Maßnahmen ergreifen – und das sowohl manuell wie automatisch.

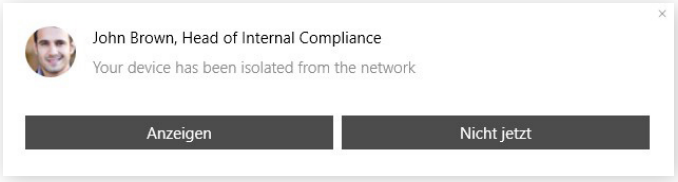

Abbildung 5 - Ultima Ratio Benachrichtigung

Wie können IT-Verantwortliche und die IT-Mannschaft nun sicherstellen, dass die Grenzen zwischen privaten und den Firmen-Applikationen im täglichen Betrieb nicht laufend überschritten werden und dass keine Firmendaten das Netzwerk unbeobachtet verlassen können oder Sicherheitslücken in nicht autorisieren Applikationen zu ungewollten Herausforderungen führen? Lösungen wie Nexthink, die Workplaces effizient analysieren, können dabei eine große Hilfe sein: Diese Software sammelt auf allen Maschinen wichtige Metriken und kann auf diese Weise auch kritische Ereignisse erkennen.

Dazu gehören beispielsweise auch Echtzeitanalysen. So werden dann alle Ereignisse in einer Datenbank abgelegt und die IT kann feststellen, welche Rechner beispielsweise einen Dienst wie Dropbox nutzen oder auf welchen Systemen immer wieder Programme abstürzen oder wo gar ungewollte Verbindungen zu unsicheren Servern im Internet aufgebaut werden. Dann kann aus der Analytics-Plattform heraus automatisiert direkt mit den jeweiligen Endanwendern Kontakt aufgenommen werden, sie werden auf das Problem aufmerksam gemacht und natürlich werden Alternativen und Lösungsvorschläge angeboten. Die Meinung der Nutzer wird entsprechend wertgeschätzt und es wird sehr viel schneller deutlich, wo „der Schuh drückt“ und was zur Nutzung der „Schatten-Programme und -Dienste“ aus dem Web geführt hat. Dabei handelt es sich nicht etwa um eine Maßnahme zur Überwachung der Arbeit der Anwender, sondern auf diese Art kann eine Verbesserung der IT und ihrer Leistung für die Endanwender im Unternehmen gezielt erreicht werden.

Mehr Erfahren

Nexthink ist ein weltweit führender Anbieter für Digital Employee Experience. Unser Produkt ermöglicht es Unternehmen, hochproduktive digitale Arbeitsplätze für ihre Mitarbeiter zu schaffen, indem sie eine optimale End-User-Erfahrung bieten. Durch eine einzigartige Kombination von Echtzeit-Analysen, Automatisierung und Mitarbeiterfeedback über alle End-Geräte hinweg hilft Nexthink IT-Teams dabei, die Anforderungen des modernen digitalen Arbeitsplatzes zu erfüllen. Erfahren Sie mehr unter www.nexthink.com.