

Was wir im Verborgenen tun

Die Gefahren von unbemerkten IT-Aktivitäten in Unternehmen



Zusammenfassung

Die Bedrohung von Unternehmen durch die Verwendung von Schatten-IT ist nicht neu, doch was wie ein unüberlegtes Versehen erscheinen mag, kann leicht zum perfekten Deckmantel für Hackerangriffe werden.

Es liegt in der Natur der Sache, dass Schatten-IT von IT-Sicherheitsteams oft nicht bemerkt wird - ein Versäumnis, das Unternehmen routinemäßig dem Risiko aussetzt, Datenschutzgesetze zu verletzen und IT-Budgets ineffizient einzusetzen. In einer Welt in der Home-Office und Fern-Arbeit eine immer größere Rolle spielen, erzeugt die inoffizielle Verwendung von Schatten-IT eine neue Bedrohungslage, die aktiv bekämpft werden muss.

Um die Verhaltensweisen, die sich hinter dem Begriff Schatten-IT verbergen und die Stimmung von Mitarbeitern, die aufgrund der Corona-Pandemie von zu Hause aus arbeiten müssen, besser zu verstehen, hat NinjaRMM die Umfrageplattform Pollfish eingesetzt, um in Deutschland insgesamt 400 Angestellte verschiedener Branchen zu befragen.

Wie sich herausstellt, kennt die Mehrheit der Befragten die Sicherheitsrichtlinien ihres Unternehmens. Jedoch umgehen die Mitarbeiter häufig diese Regeln, indem sie eine ganze Reihe verschiedener Geräte verwenden, wie Festplatten und Smartphones oder durch den Einsatz digitaler Tools, wie Kommunikations- und Unternehmenssoftware. Die auf den Umfrageergebnissen basierenden Empfehlungen legen nahe, dass häufige Sicherheitsschulungen in Verbindung mit klaren Richtlinien und einer reibungslos ineinandergreifenden IT-Infrastruktur dabei helfen können, die Gründe zu minimieren oder ganz zu beseitigen, aus denen sich Mitarbeiter überhaupt erst zur Nutzung inoffizieller Geräte und Softwareanwendungen hinreißen lassen.

Die Auswirkungen von Fernarbeit auf die Schatten-IT

Neue Untersuchungen von NinjaRMM zeigen, dass viele Mitarbeiter die etablierten Sicherheitsrichtlinien ihrer Organisation umgehen, weil sie ihnen zu umständlich sind.

Mitarbeiter an Fern-Arbeitsplätzen nannten drei Hauptgründe, warum sie Sicherheitsrichtlinien umgehen:

- 1** Die Sicherheitsrichtlinien sind zu restriktiv und beeinträchtigen ihre Produktivität.
- 2** Ihre IT-Abteilung reagiert zu langsam auf ihre Anfragen
- 3** Es ist einfacher, persönliche Konten zur Verwaltung von Arbeitsdokumenten zu verwenden

Wenn man sich darauf verlässt, dass Mitarbeiter an Fern-Arbeitsplätzen immer die Regeln befolgen, wird dies immer zu Sicherheitslücken führen, aber konsequente und häufige Sicherheitsschulungen können dem entgegenwirken.

70%

der Mitarbeiter an Fern-Arbeitsplätzen hatten Zugang zu Sicherheitsschulungen

66%

der Mitarbeiter an Fern-Arbeitsplätzen erhielten in den letzten 6 Monaten eine Sicherheitsschulung

42%

der Mitarbeiter an Fern-Arbeitsplätzen meinten, sie müssten die Sicherheitspolitik ihrer Organisation umgehen, um ihre Arbeit erledigen zu können

Einzelne Mitarbeiter geben mehr von ihrem eigenen Geld für digitale Werkzeuge und Hardware aus, was auf eine Wissenslücke in der IT hinweist und darauf, was ihre Mitarbeiter benötigen, um erfolgreich zu sein.

44%

der Mitarbeiter an Fern-Arbeitsplätzen geben Geld für digitale Tools und Hardware aus.

61%

der Mitarbeiter an Fern-Arbeitsplätzen gaben zwischen 11 und 50 Euro pro Monat für digitale Werkzeuge und Hardware aus

Die Zeit, die Mitarbeiter mit IT-Fragen verbringen, ist seit der Zeit im Home-Office gestiegen.

64%

der Mitarbeiter an Fern-Arbeitsplätzen verbringen 2 oder mehr Stunden pro Woche mit IT-Problemen.

Empfehlungen, um das IT-Management aus dem Schatten zu holen

Die größte Herausforderung bei der Bekämpfung von Schatten-IT und der Reduzierung der damit verbundenen Risiken ist der Aufbau einer Sicherheitskultur in der Organisation. Im Folgenden finden Sie einige Empfehlungen, die IT- und Geschäftsleiter zur Förderung einer integrativen Sicherheitskultur geben können:

1

Überprüfen Sie die am häufigsten verwendeten digitalen Tools und Hardware von Mitarbeiter an Fern-Arbeitsplätzen, um festzustellen, ob die aktuelle Sicherheitspolitik nicht ihren Bedürfnissen entspricht

2

Überprüfen Sie etablierte Sicherheitsrichtlinien und suchen Sie nach Wegen, um die Spannung zwischen Mitarbeitern und IT zu verringern

3

Organisieren Sie regelmäßige Sicherheitsschulungen zu den wichtigsten Bedrohungen, denen Mitarbeiter an Fern-Arbeitsplätzen wahrscheinlich ausgesetzt sind, wie Phishing und Malware

4

Richten Sie klare Kommunikationswege zwischen Mitarbeiter an Fern-Arbeitsplätzen und IT-Mitarbeitern ein, um ein größeres Bewusstsein für IT-Fragen und die Übernahme der Sicherheitsrichtlinien zu fördern

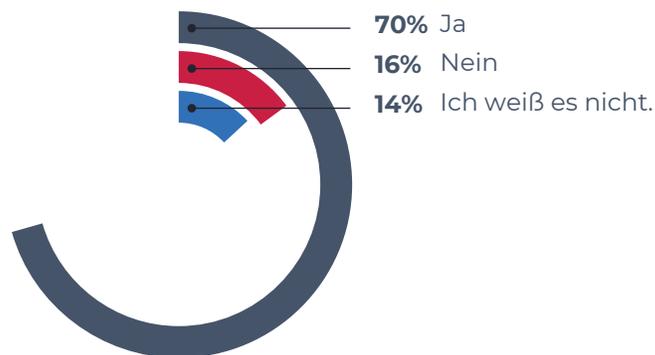
5

Kommunizieren Sie IT-Probleme, Bedürfnisse und Erkenntnisse regelmäßig an das Führungsteam, damit sich das Unternehmen angemessen auf sich entwickelnde Bedrohungen einstellen kann

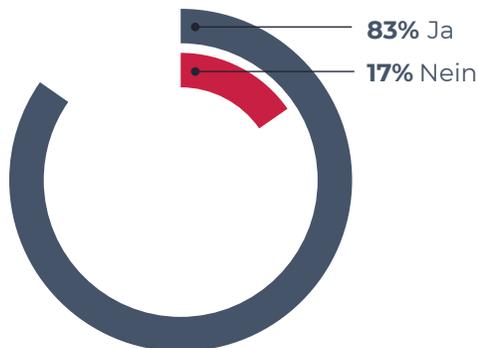
Kommunizieren Sie Ihre Sicherheitsrichtlinien klar und verständlich

Die Gewährleistung einer hohen Sicherheit setzt voraus, dass die Mitarbeiter die IT-Sicherheitsrichtlinien ihrer Organisation kennen. Sie müssen genau wissen, was zu tun ist, wenn sie bei der Arbeit auf ein neues Tool oder Gerät stoßen. Die Teilnehmer unserer Umfrage waren zu 83% mit den IT-Sicherheitsbestimmungen ihres Unternehmens vertraut und 70% von ihnen hatten Zugang zu Sicherheitsschulungen.

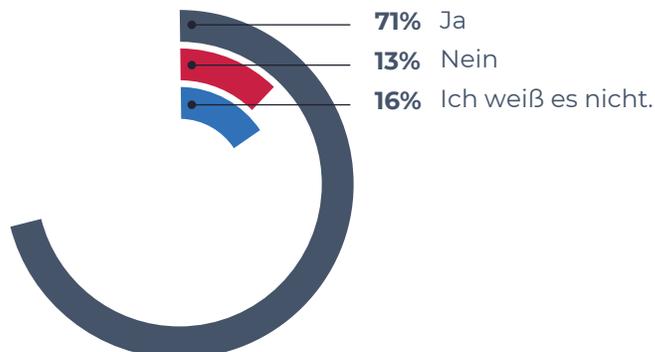
Bietet Ihr Unternehmen Schulungen über die Bedeutung der Einhaltung bewährter Sicherheitsverfahren an?



Sind Sie mit den IT-Sicherheitsrichtlinien Ihres Unternehmens vertraut?



Deckt die IT-Sicherheitsrichtlinie Ihres Unternehmens Dinge wie die Verwendung nicht genehmigter Software, Hardware oder Cloud-Dienste auf Arbeitsgeräten ab?

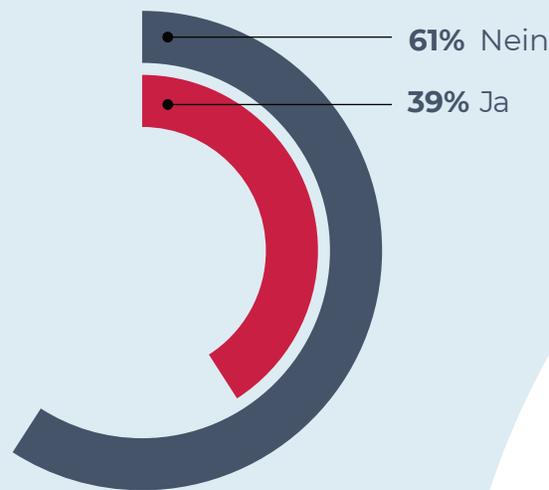


Natürlich sind der Zugang zu Trainings und die tatsächliche Durchführung dieses Trainings zwei verschiedene Dinge. Während wir feststellen konnten, dass 66% der Befragten innerhalb der letzten 6 Monate eine Schulung erhalten haben, gab es auch 34%, die seit mehr als einem Jahr nicht geschult oder teilweise noch nie in Sicherheitsfragen unterwiesen worden sind. Die letzten 6 Monate haben das Nutzerverhalten von Mitarbeitern, vor allem an Fern-Arbeitsplätzen, von Grund auf verändert. Dieser Wandel verlangt von IT-Sicherheitsexperten, dass sie sofort Maßnahmen ergreifen und Mitarbeiter über die neuesten Bedrohungen aufklären. Angesichts des enormen Gefahrenpotentials lohnt sich das Investment in regelmäßige und wiederkehrende Schulungen der Mitarbeiter, welches sich in jedem Fall auszahlen wird.

34% erhielten innerhalb des letzten Jahres oder länger keine Sicherheitsschulung oder haben nie eine solche Schulung erhalten



Haben Sie jemals das Gefühl, dass Sie die etablierten Sicherheitsrichtlinien und -verfahren Ihres Unternehmens umgehen müssen, um Ihre Arbeit tun zu können?



Im Mittelpunkt jeder Sicherheitsrichtlinie für Mitarbeiter an Fern-Arbeitsplätzen sollte eine klare Regelung stehen, welche Anwendungen, Cloud-Dienste und Hardware verwendet werden dürfen, damit sich inoffizielle IT-Infrastrukturen gar nicht erst ausbreiten. 71% der Befragten geben an, dass die Sicherheitsrichtlinien ihrer Organisation Problematiken wie die Verwendung nicht genehmigter Software, Cloud-Dienste oder Hardware abdecken. Angesichts der Tatsache, dass 39% der Mitarbeiter an Fern-Arbeitsplätzen sagen, dass sie die Sicherheitsrichtlinien umgehen müssen, um ihre Arbeit erledigen zu können, sollten sich IT-Sicherheitsexperten jedoch nicht darauf verlassen, dass die Endbenutzer sich immer nach den Vorgaben richten werden.

39% der Mitarbeiter an Fern-Arbeitsplätzen meinten, sie müssten die Sicherheitspolitik ihrer Organisation umgehen, um ihre Arbeit erledigen zu können



25% würden die Sicherheitsrichtlinien ihres Unternehmens umgehen, falls diese zu restriktiv für ihre Produktivität sind



Was sind einige der Gründe, warum Sie die IT-Sicherheitsrichtlinien Ihres Unternehmens umgehen würden?

Die IT-Richtlinien sind zu restriktiv für meine Produktivität.

25%

Die IT-Richtlinien sind schwer zu verstehen

22%

Die IT-Abteilung war zu langsam, um neue Software oder digitale Tools zu überprüfen

24%

Es ist bequemer, persönliche Konten zur Verwaltung von Arbeitsdokumenten zu verwenden

22%

Mir waren die IT-Sicherheitsrichtlinien des Unternehmens nicht bekannt

9%

Es gibt keine IT-Sicherheitsrichtlinien

5%

Ich würde niemals die IT-Sicherheitspolitik des Unternehmens umgehen

35%

0 5 10 15 20 25 30 35



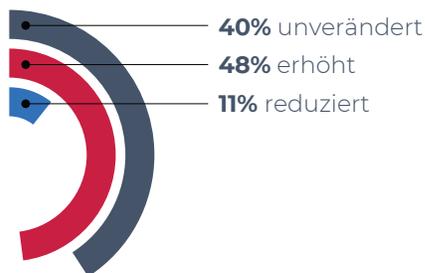
Es ist äußerst beunruhigend zu sehen, dass eine große Zahl von Menschen das Gefühl hat, die Sicherheitspolitik ihrer Organisation umgehen zu müssen", sagte Lewis Huynh, Chief Security Officer von NinjaRMM.

"Abgesehen von den Sicherheitsbedenken, die sich aus der Verletzung von Unternehmensrichtlinien ergeben, spiegelt dies ein Versagen der Führung wider. Es zeigt, dass sie entweder nicht verstehen, was nötig ist, damit ihre Teams ihre Arbeit erledigen können, oder dass sie nicht in die Ressourcen investieren wollen, die ihre Mitarbeiter produktiver machen können. Dieses Verhalten führt zu Zeit- und Ressourcenverlusten sowie nicht genutztem Potential."

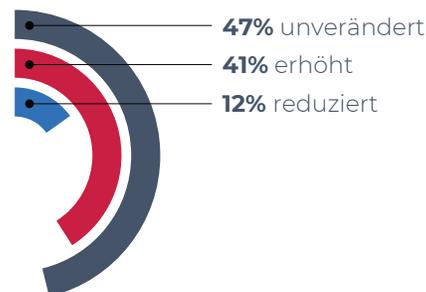
Empfehlungen, um das IT-Management aus dem Schatten und ans Licht zu bringen

Für einige Beschäftigte ging die Verlagerung auf Fernarbeit Hand-in-Hand mit einem Anstieg der Zahl von Geräten und Software- oder Cloud-Diensten einher, die sie zur Verrichtung ihrer Arbeit benötigten. Insgesamt 41% von ihnen geben an, dass sich die Anzahl der von ihnen verwendeten Geräte erhöht habe, während 48% von einem Anstieg der Anzahl an Software- oder Cloud-Diensten berichten.

Hat sich die Menge an Software oder Cloud-Diensten, die Sie für Ihre Arbeit nutzen, seit Sie von zu Hause aus arbeiten, erhöht, verringert oder ist sie gleich geblieben?



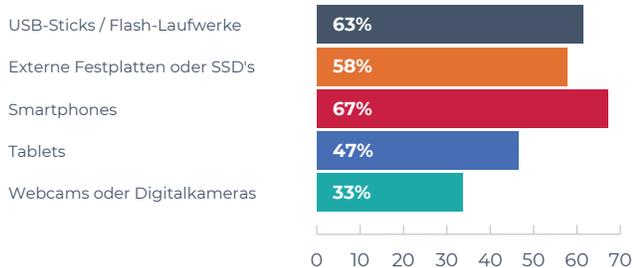
Hat sich die Zahl der Geräte, die Sie bei der Arbeit benutzen, seit Sie von zu Hause aus arbeiten, erhöht, reduziert oder ist sie gleich geblieben?



Die Ausbreitung von Apps kann zu einem großen Problem für die Cybersicherheit werden, insbesondere wenn IT-Abteilungen nicht über die von den Mitarbeitern verwendeten Tools Bescheid wissen und wenn die Mitarbeiter sich nicht um Updates und Patches für die verwendete Software kümmern. Dieses Nutzerverhalten kann Cyberkriminellen Tür und Tor zum Unternehmen öffnen. Auch wenn die allermeisten Endbenutzer nicht böswillig handeln, der vermehrte Einsatz unüberwachter digitaler sowie physischer Hilfsmittel bei der Arbeit von Fern-Arbeitsplätzen bringt möglicherweise hochgefährliche neue Schwachstellen für die Integrität der Unternehmenssicherheit mit sich.

Unter den Befragten, die inoffizielle Hardware, Software oder Cloud-Dienste verwendeten, lassen sich große Unterschiede in der Art der unüberwachten digitalen und physischen Hilfsmittel feststellen. In der Kategorie Hardware sind Smartphones (mit 67%), USB-Flash-Laufwerke (mit 63%) und externe Festplatten oder SSDs (mit 58%) am weitesten verbreitet. Bei Software- und Cloud-Diensten werden Audio- und Videosoftware (mit 52%), Kommunikationssoftware (mit 46%) und Geschäfts- und

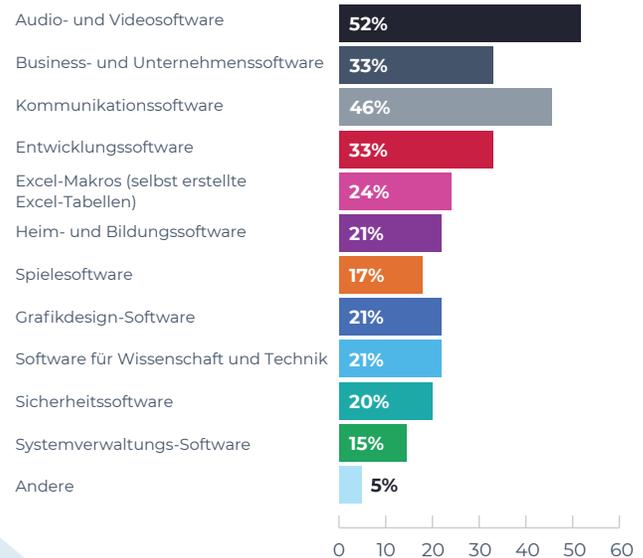
Welche Geräte verwenden Sie, die von Ihrem Unternehmen oder Ihrer IT-Abteilung nicht zugelassen sind? Wählen Sie alle zutreffenden Geräte aus:



Das Unterbinden von inoffiziellen Anwendungen sollte jedem IT-Sicherheitsexperten ein Anliegen sein. Viele Mitarbeiter scheinen ihre Arbeitsgeräte zur persönlichen Unterhaltung und Kommunikation zu nutzen, denn 18% haben Spielsoftware auf ihrem Arbeitsgerät installiert. Diese Anwendungen für den Privatgebrauch haben nicht das gleiche Sicherheitsniveau wie ihre Pendant auf Unternehmensebene und könnten zu einer Quelle von Datenlecks oder Datenmissbrauch werden.

"Jegliche inoffizielle Anwendung auf Arbeitsgeräten ist problematisch", betont Lewis Huynh von NinjaRMM. "Die Wahrscheinlichkeit ist geringer, dass diese Anwendungen gepatcht werden und dadurch sind die Mitarbeiter an Fern-Arbeitsplätzen einem größeren Risiko ausgesetzt. Bei all den Bedrohungen, denen Unternehmen ausgesetzt sind, ist eine freizügige Haltung gegenüber arbeitsfremder Software ein unnötiges Risiko, das es einzudämmen gilt."

Welche Art von Software oder Cloud-Diensten verwenden Sie auf Ihren Arbeitsgeräten, die nicht von Ihrem Unternehmen oder Ihrer IT-Abteilung genehmigt wurden? Wählen Sie alle zutreffenden aus:



17% der Mitarbeiter an Fern-Arbeitsplätzen haben Spielsoftware auf ihren Arbeitsgeräten installiert



Versteckte Kosten und verlorene Arbeitszeit bei Angestellten im Home-Office

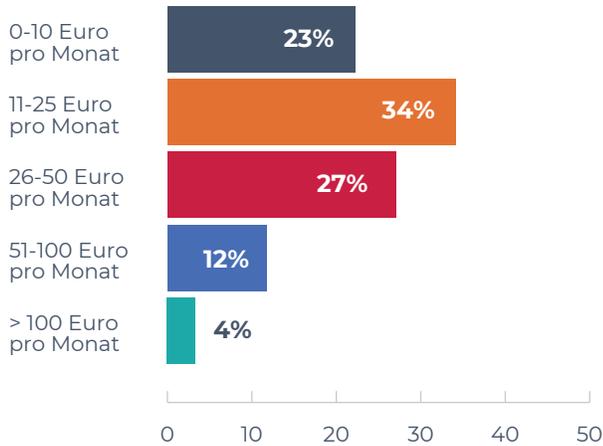
Ein zentrales Anliegen jedes IT-Spezialisten ist die Budgetkontrolle. Aber das Gleichgewicht zwischen den Bedürfnissen der Firma und den Bedürfnissen der Mitarbeiter im Home-Office zu finden, ist eine schwierige Aufgabe, Schatten-IT erschwert das Ganze noch zusätzlich. Wenn Mitarbeiter an Fern-Arbeitsplätzen unüberwachte Geräte und Anwendungen verwenden, können IT-Abteilungen nicht wissen, welche Tools die Mitarbeiter tatsächlich benötigen. So kann es leicht passieren, dass Ressourcen in unproduktive oder nicht genutzte Tools investiert werden.

44% haben eigenes Geld für arbeitsrelevante Hardware, Software oder Cloud-Dienste ausgegeben



Wir fanden heraus, dass 44% der Befragten eigenes Geld für Hardware, Software oder Cloud-Dienste für die Arbeit ausgegeben haben. Von dieser Gruppe geben 34% an, dass sie zwischen 11 und 25 Euro pro Monat für digitale oder physische Hilfsmittel ausgeben. Diese Informationen benötigen IT-Abteilungen, um überhaupt auf einen Bedarf unter den Mitarbeitern aufmerksam zu werden und eine sichere Alternative anbieten zu können.

Wenn ja, wie viel geben Sie pro Monat für Hardware, Software oder Cloud-Dienste aus, die für die Arbeit genutzt werden?

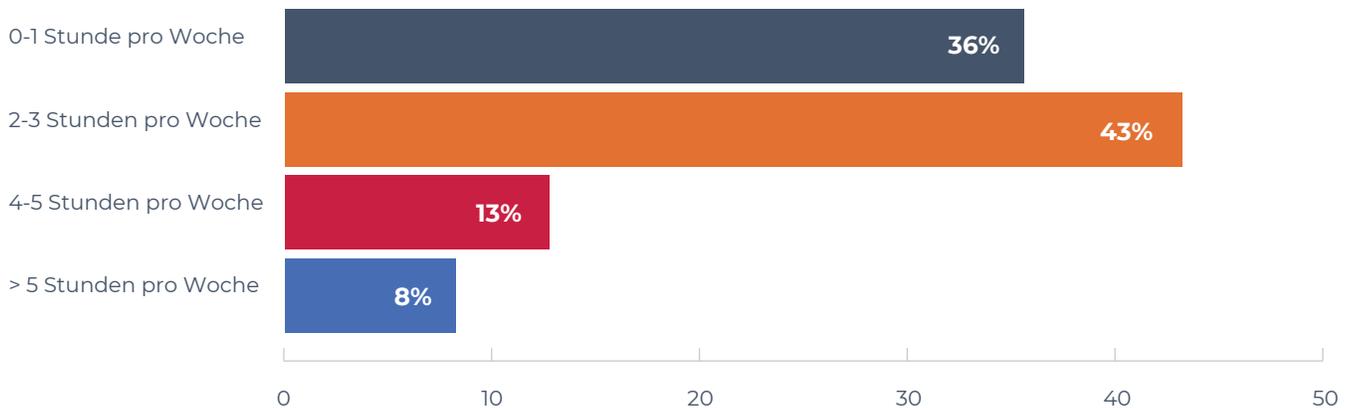


Darüber hinaus stellten wir fest, dass 46% der Mitarbeiter an Fern-Arbeitsplätzen mehr Zeit für IT-Fragen aufwenden, seit sie aufgrund der Corona-Pandemie gezwungen sind, verstärkt von zu Hause aus zu arbeiten. 64% der Mitarbeiter im Home-Office geben an, dass sie zwei Stunden oder mehr pro Woche für IT-Fragen aufwenden, wodurch sich ihre Produktivität für das Unternehmen

46% der Mitarbeiter an Fern-Arbeitsplätzen verbringen aufgrund der Corona-Pandemie mehr Zeit mit der Lösung von IT-Fragen als direkte Folge ihrer neuen Tätigkeit aus dem Home-Office



Wie viel Zeit verbringen Sie pro Woche außerhalb Ihrer normalen Aufgaben mit IT-Fragen?

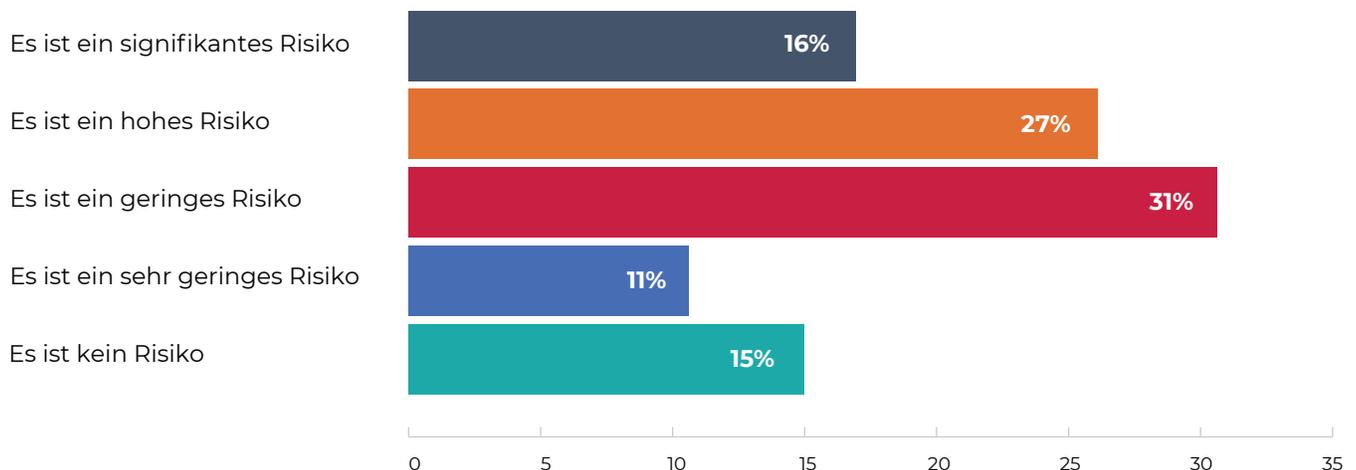


Wie nehmen die Betroffenen die von Schatten-IT ausgehende Gefahr selbst wahr?

Schatten-IT kann schwerwiegende Auswirkungen auf Unternehmen haben. Gerade jetzt, da viele Mitarbeiter von zu Hause aus arbeiten, ist die Angriffsfläche exponentiell größer geworden. Von Datenlecks und Datendiebstahl bis hin zu nicht gepatchten Anwendungen auf fernverwalteten Endpunkten - die Bedrohung durch Schatten-IT war noch nie so groß wie jetzt.

Wir fanden heraus, dass 57% der Befragten der Meinung sind, dass die Nutzung unüberwachter Hardware, Software oder von Cloud-Diensten nur wenig oder überhaupt nicht riskant sei. In Anbetracht der von uns diskutierten Gefahren von inoffiziell verwendeter Schatten-IT ist dies ein alarmierender Standpunkt, der darauf hindeutet, dass IT-Sicherheitsteams mehr tun müssen, um die Mitarbeiter über die Risiken aufzuklären.

Auf einer Skala von 1 bis 5, wie hoch schätzen Sie das Risiko ein, nicht genehmigte Software, Hardware oder Cloud-Dienste für Arbeitszwecke zu nutzen?



Schlussfolgerungen und Empfehlungen

In der neuen Arbeitswirklichkeit, mit stark dezentralisierten Arbeitsplätzen, in der wir uns befinden, stellen IT-Sicherheitsexperten vermehrt fest, dass Sicherheitslücken, die früher klein und unbedeutend erscheinen mochten, sich nun zu ernsthaften Bedrohungen entwickelt haben. Diese müssen identifiziert und entschärft werden. Unsere Umfrage ergab, dass Schatten-IT für Unternehmen eine Bedrohung darstellt, die sich sowohl negativ auf die Produktivität der Mitarbeiter, den Datenschutz und die Datensicherheit als auch auf das Unternehmensbudget selbst auswirkt.

Das Unterbinden von Schatten-IT sollten Sie zu einer Priorität für jedes Führungsteam machen. Unsere Untersuchungsergebnisse deuten darauf hin, dass viele Führungskräfte die Gefahren der Schatten-IT nicht verstehen oder ihnen nicht bewusst ist, welche Technologie die Mitarbeiter für ihre Arbeit benötigen. Indem sie die Schatten-IT unterbinden, können Führungskräfte dazu beitragen, neue Wachstumsbereiche für das Unternehmen zu erschließen und gleichzeitig ein sich ständig änderndes IT-Budget zu verwalten.

Betrachtet man die Gründe, warum Mitarbeiter unerlaubt Geräte und Anwendungen einsetzen, wird deutlich, dass eine konstante Kommunikation zwischen IT-Abteilungen und den Mitarbeitern stattfinden muss, um an den Konfliktlinien zu arbeiten. Schatten-IT Strukturen entstehen in der Regel, wenn es in einer Organisation zu viel Bürokratie gibt, die das Arbeiten erschwert. Wenn IT-Abteilungen neue, leichter zugängliche Prozesse ins Auge fassen, können sie dem Einzelnen Arbeitserleichterungen anbieten und gleichzeitig mehr Sicherheit für das gesamte Unternehmen gewährleisten.

Letztlich hängt die Aufrechterhaltung der Sicherheit von Unternehmen in einem dezentralisierten Arbeitsumfeld von der Pflege persönlicher Beziehungen ab und dem Vertrauen darauf, dass die einzelnen Teammitglieder die Richtlinien befolgen. Indem IT-Teams mit den dezentral arbeitenden Mitarbeitern proaktiv über Schwierigkeiten und Unzufriedenheiten diskutieren, können sie dazu beitragen, die Verwendung von Schatten-IT einzudämmen.