Dashlane-Bericht über den Stand der Sicherheit von Zugangsdaten

Wie KI und die sich entwickelnde Belegschaft die Bedrohung durch Sicherheitsverletzungen bei Zugangsdaten verstärken können

DASHLANE

Inhaltsverzeichnis

Einführung
Die gewaltige Herausforderung in einer sich wandelnden Cybersicherheitslandschaft 03

Abschnitt 1
KI-gestütztes Phishing: Die unmittelbare Gefahr für Ihre Sicherheit 04

Abschnitt 2
Traditionelle Ansätze für Sicherheitsstrategien scheitern ann moderne Belegschaften nicht gut 05

Abschnitt 3
Schatten-IT: Das versteckte Risiko für die Sicherheit Ihres Unternehmens 08

Abschnitt 4
Die Sicherheit von Zugangsdaten liegt in den Händen überlasteter IT-Teams 09

Fazit
Neue Lösungen für neue Herausforderungen 10

EINFÜHRUNG

Die gewaltige Herausforderung in einer sich verändernden Cybersicherheitslandschaft

In Angesicht der wachsenden Herausforderungen durch eine KI-getriebenen Welt, denen Unternehmen gegenüberstehen, hat sich die Landschaft der Cybersicherheitsbedrohungen dramatisch verändert, wobei hybride Arbeit eine weitere Komplexitätsebene hinzufügt.

Künstliche Intelligenz (KI) hat Risiken hinsichtlich der Passwortsicherheit erhöht, da sie großflächige, nun hocheffektive Phishing-Angriffe ermöglicht, die traditionelle Verteidigungsmaßnahmen wie die regelbasierte Bedrohungserkennung umgehen. Unterdessen hat ein verändertes Verhalten am Arbeitsplatz, einschließlich der Vermischung privater und beruflicher Geräte, die Angriffsfläche für Hacker vergrößert. Schatten-IT vergrößert weiter Schwachstellen in Unternehmen.

IT-Führungskräfte stehen jetzt vor der gewaltigen Herausforderung, mit diesen eskalierenden Bedrohungen umgehen zu müssen. Sie balancieren zwischen den Anforderungen an Schulungen, organisatorischen Veränderungen und Compliance-Anforderungen und sehen sich gleichzeitig dem wachsenden Risiko einer Sicherheitsverletzung gegenüber.

> „Die Sicherheit von Zugangsdaten steht wirklich an einem Wendepunkt“,

Viele IT-Teams sehen die Grenzen traditioneller Ansätze und suchen dringend nach umfassenderen, proaktiven Lösungen, um diesen wachsenden Risiken gerecht zu werden.

Um zu verstehen, wie sich die Last der Verwaltung von Zugangsdaten auf IT-Teams auswirkt, haben wir sowohl Mitarbeitende als auch IT-Führungskräfte befragt. Der vorliegende, auf diesen Umfragen basierenden Bericht untersucht den aktuellen Stand hinsichtlich der Sicherheit von Zugangsdaten in Unternehmen. Außerdem sprechen wir darüber, wie Passwortmanager sich von einer passiven zu einer proaktiven Risikoerkennung entwickeln müssen, um Datenschutzverletzungen zu verhindern und IT-Teams sowie deren Kollegen von der Sicherheit zu unterstützen.

Methodik

sagt Frederic Rivain, Chief Technology Officer von Dashlane. „Der durchschnittliche Mitarbeiter sieht sich oftmals an nur einem Tag mehreren Phishing-Versuchen ausgesetzt. IT-Teams benötigen die Tools, um Mitarbeitende zu überwachen, zu unterstützen und sie dazu zu befähigen, Risiken zu minimieren. Die passwortlose Zukunft verspricht zwar, einen Großteil der durch Passwörter verursachten Risiken und Schmerzen zu beseitigen, aber da sind wir noch nicht.“

Die Ergebnisse basieren auf einer von Dashlane in Auftrag gegebenen und von DKC Analytics durchgeführten wissenschaftlichen Umfrage unter zufällig ausgewählten 1.000 arbeitenden Erwachsenen und 500 IT-Entscheidungsträgern in den USA.

Copyright © 2025 Dashlane

Teil 1

KI-gestütztes Phishing: Die unmittelbare Gefahr für Ihre Sicherheit.

Mithilfe von KI können Cyberkriminelle auf die Daten Ihres Unternehmens zugreifen. Dadurch ist es für sie jetzt einfacher denn je, Phishing- und Spear-Phishing-Angriffe in großem Umfang durchzuführen, ohne viel investieren zu müssen. Dank der neuen Generation an Phishing-Kits, einschließlich solcher, die Tools wie EvilProxy nutzen und große Sprachmodelle sowie generative KI enthalten, können Angreifer nun hochgradig personalisierte, überzeugende Nachrichten versenden. Zudem greifen diese Kits auf fortschrittliche Taktiken, einschließlich Deepfakes und KI-generierter Inhalte, zurück, sodass die Betrugsmaschen immer ausgeklügelter werden.

IT-Führungskräfte und Mitarbeitende berichten, dass sich mit dem Aufstieg von KI und der daraus resultierenden Komplexität von Phishing-Angriffen das Risiko für die Sicherheit von Zugangsdaten erhöht hat:

Unsere Daten spiegeln auch die wachsende Bedrohung durch Phishing wider:

88 % der **Mitarbeitenden** sagen, dass es vermehrt Phishing-Versuche gibt, die auf Ihr Unternehmen abzielen

74%

der IT-Führungskräfte sagen, dass KI eine erhöhte Bedrohung für die Passwortsicherheit darstellt

60%

der Mitarbeitenden stimmen zu, dass KI eine erhöhte Bedrohung für die Passwortsicherheit darstellt

80 %

der **IT-Führungskräfte** sagen, dass es vermehrt Phishing-Versuche gibt, die auf ihr Unternehmen abzielen

84 %

der **IT-Führungskräfte** berichten von einem Anstieg des Phishing-Volumens, der Komplexität oder von beidem

Abschnitt 2

Traditionelle Ansätze für Sicherheitsstrategien scheitern an modernen Belegschaften

Traditionelle Sicherheitsstrategien, die auf dem Schutz eines gut definierten Netzwerkperimeters und dem Einsatz von Sicherheitsschulungen als zentrales Verteidigungsmittel basieren, scheitern am modernen Arbeitsplatz.

Remote- und hybride Arbeit gestalten die Cybersicherheitslandschaft weiter um und bringen neue Risiken mit sich, da bei Mitarbeitenden die

Ein Unternehmen mit 1.000 Mitarbeitenden müsste jährlich 12.000 bis 24.000 USD für Online-Basisschulungen ausgeben. Größeren Unternehmen (über 10.000 Mitarbeitende) könnten Kosten in Höhe von Hunderttausenden oder sogar Millionen pro Jahr entstehen, insbesondere wenn sie umfassende Schulungen, Phishing-Simulationen und konformitätsorientierte Schulungen organisieren.

Grenzen zwischen privaten und geschäftlichen Geräten verschwimmen. Die erweiterte Angriffsfläche – aufgrund schwacher Passwortverfahren und unsicherer Heimnetzwerke – ist zu einem perfekten Einfallstor für Cyberkriminelle geworden.

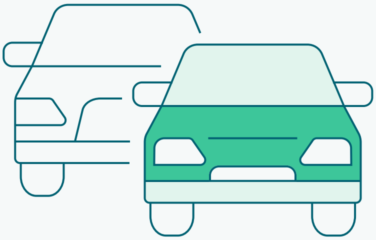
Oft verbinden sich Mitarbeitende über unsichere WLAN-Netzwerke mit Unternehmenssystemen. Vielen dieser Netzwerke fehlen angemessene Sicherheitsmaßnahmen wie aktualisierte Router, VPNs oder starke Passwörter. Ohne einen klar definierten zu verteidigenden Perimeter stellt der eigene Schutz Unternehmen jetzt vor einer deutlich komplexeren Herausforderung.

Sicherheitsbewusstsein und Schulungsprogramme sind gängige Tools zur Minderung menschlicher Risiken, einschließlich Phishing. Großunternehmen investieren viel Zeit und Geld in sie – aber Mitarbeitende erkennen nicht den gleichen Nutzen in diesen Schulungen.

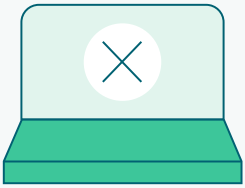
Zusätzliche Sicherheitsschulungen wirken sich auch auf die Produktivität aus. 57 % der befragten IT-Führungskräfte sagen, dass Mitarbeitende Sicherheitsschulungen als lästig empfinden.

Copyright © 2025 Dashlane

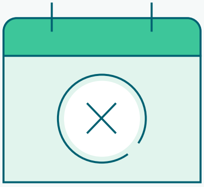
43 % der Mitarbeitenden würden extreme Maßnahmen ergreifen, um Sicherheitsschulungen zu vermeiden



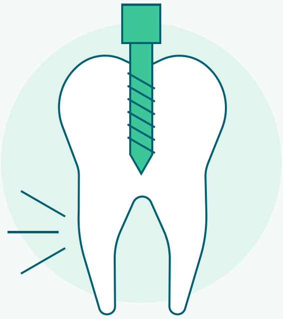
22% würden lxieber zu den Hauptverkehrszeiten im Stau stecken



13% würden lieber ganz auf Computer verzichten, wenn sie dadurch nicht an einer Schulung teilnehmen müssten



15% würden lieber auf einen Urlaubstag verzichten, wenn sich dadurch die Schulung vermeiden ließe



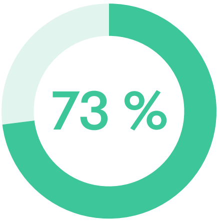
11% Würden lieber einen Root-Kanal haben, als an einer Schulung teilzunehmen

IT-Führungskräfte sind sich einig: 51 % glauben, dass Mitarbeitende in ihrem Unternehmen Sicherheitsschulungen als lästig empfinden. Diese Übereinstimmung ist ein klares Zeichen dafür, dass Sicherheitsschulungen nicht die gewünschten Ergebnisse hinsichtlich des Schutzes von Unternehmen vor menschlichen Schwachstellen erreichen.

Copyright © 2025 Dashlane

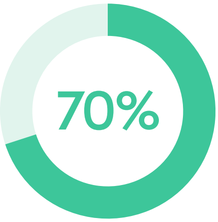
IT-Führungskräfte berichten von drei gängigen Passwortproblemen.

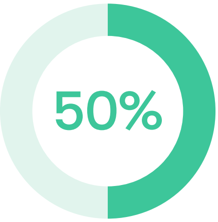
Eine schlechte Passworthygiene von Mitarbeitenden erhöht die Risiken. Fast alle IT-Führungskräfte (96 %) berichten, dass sie sich mit Problemen im Zusammenhang mit Zugangsdaten beschäftigen müssen. Die drei häufigsten Probleme sind:



Mitarbeitende vergessen Passwörter und/oder müssen ein Passwort zurücksetzen

Mitarbeitende erstellen schwache und anfällige Passwörter.





Mitarbeitende geben Passwörter mit ungesicherten Methoden (wie Slack oder E-Mail) weiter

Diese schlechten Gewohnheiten führen zu greifbaren Verlusten. IT-Führungskräfte geben an, dass ihr Unternehmen wegen schwacher oder gefährdeter Passwörter Opfer eines Diebstahls von geistigem Eigentum wurde (37 %) und wegen gefährdeter Konten Geld gestohlen werden konnte (19 %).

Passwortbezogene Probleme sind für Unternehmen nicht nur die Ursache von Sicherheitsverletzungen, sondern führen auch zu erheblichen Betriebskosten. Forrester Research schätzt, dass jedes Zurücksetzen von Passwörtern unter Einberechnung der von IT-Mitarbeitenden aufgewendeten Zeit und der Produktivitätsverluste rund 70 USD kostet. Darüber hinaus geht es bei bis zu 40 % der Helpdesk-Anrufe um Passwortprobleme, was einen erheblichen Supportaufwand bedeutet. Zudem verbringen Mitarbeitende durchschnittlich 11 Stunden pro Jahr damit, Passwörter zurückzusetzen, was deren Produktivität zusätzlich beeinträchtigt. Alles zusammengerechnet geben Unternehmen geschätzt durchschnittlich 5,2 Millionen USD jährlich für passwortbezogenen Support und Infrastruktur aus.

Copyright © 2025 Dashlane

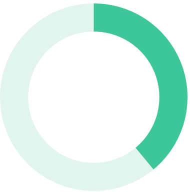
Abschnitt 3

Schatten-IT: Das versteckte Risiko für die Sicherheit Ihres Unternehmens

Schatten-IT birgt erhebliche Risiken für Unternehmen. Das Problem wird noch größer, da die Akzeptanz generativer KI-Tools durch Mitarbeitende sprunghaft zunimmt. Diese Tools sind besonders riskant, da sie mit viel mehr Systemen und Apps in einem Unternehmen verbunden sind und riesige Mengen an sensiblen Daten verarbeiten können.

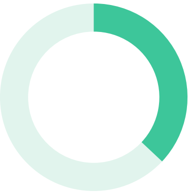
Dieses Risiko wird nicht verschwinden. Einige dieser Apps tragen dazu bei, dass Mitarbeitenden produktiver sind und helfen dem Unternehmen, seine Ziele zu erreichen.

Unsere Daten zeigen, dass die Bedrohung durch Schatten-IT real ist:



39 %

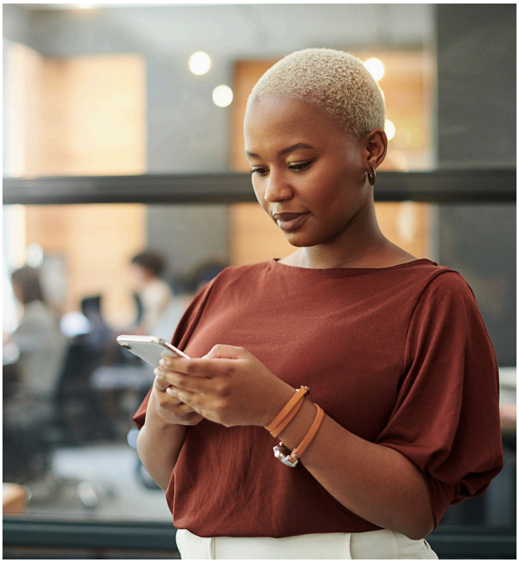
der Mitarbeitenden Apps auf Arbeitsgeräten installiert haben, die nicht von ihrem Unternehmen verwaltet werden



37 %

der Unternehmens-Apps nicht Single Sign-on (SSO) nutzen

Schatten-IT verursacht zahlreiche Probleme, einschließlich einer erhöhten Angriffsfläche und potenzieller Compliance-Verstöße.



Ohne Transparenz bei den Geräten, Anwendungen und Diensten, die auf Unternehmensressourcen zugreifen, können IT-Teams Unternehmensdaten nicht sichern und sicherstellen, dass nur autorisierte Benutzer auf sensible Daten und Systeme zugreifen. Diese fragmentierte Transparenz macht es schwierig, Bedrohungen von extern und intern zu erkennen.

Daher macht Schatten-IT Unternehmen letztendlich anfällig für Cyberangriffe und Datenverlust oder -kompromittierung. Der potenzielle Schaden geht jedoch weit über finanzielle Verluste hinaus, denn zumeist leidet auch der Ruf des Unternehmens, der sich nur mit viel Zeit und Aufwand wiederherstellen lässt.

Copyright © 2025 Dashlane

Abschnitt 4

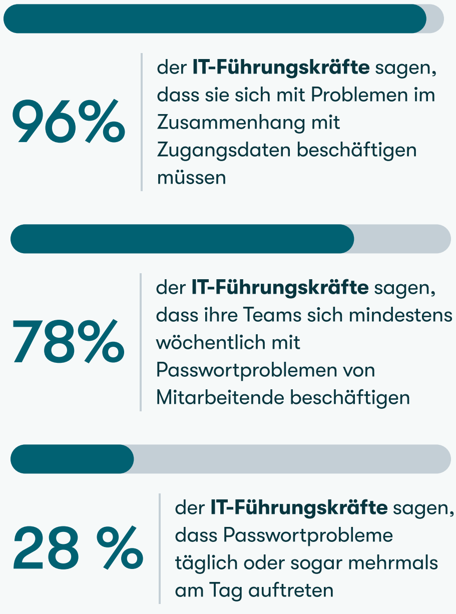
Die Sicherheit von Zugangsdaten liegt in den Händen überlasteter IT-Teams

Burnout ist unter IT-Teams zu einer Epidemie geworden. Untersuchungen zeigen, dass 58 % der IT-Mitarbeitende berichten, mit ihren täglichen Aufgaben überfordert zu sein. Darüber hinaus berichtet der durchschnittliche IT-Mitarbeiter, dass er nur 85 % der täglich eingegangenen Tickets bearbeiten kann.

Unsere Daten zeigen, dass die manuelle Verwaltung von Zugangsdaten diese Belastung erheblich erhöht. Wie bereits erwähnt, geben 96 % der IT-Führungskräfte an, dass sie sich mit Problemen im Zusammenhang mit Zugangsdaten beschäftigen müssen, wobei das Zurücksetzen von Passwörtern und schwache Passwörter die häufigsten Probleme darstellen.

Diese Probleme kosten viel Zeit und tragen erheblich zu Burnouts bei. Mehr als drei Viertel (78 %) der IT-Führungskräfte geben an, dass ihre Teams sich mindestens wöchentlich mit Passwortproblemen von Mitarbeitenden beschäftigen. Bei 28 % treten Passwortprobleme täglich oder sogar mehrmals am Tag auf.

Darüber hinaus müssen IT-Teams noch andere Aufgaben im Rahmen ihrer Arbeit erledigen: Durchführung von Schulungen, Anpassung von Prozessen an organisatorische Veränderungen, Erfüllung der Erwartungen von Führungskräften, Adressieren der Bedrohung durch Sicherheitsverletzungen und mehr. Hinzu kommen noch die zunehmenden Risiken im Zusammenhang mit Zugangsdaten und die Auswirkungen der Abneigung von Mitarbeitenden gegen Sicherheitsschulungen, die zusätzlich zur Überforderung von IT-Teams beitragen.



96% der **IT-Führungskräfte** sagen, dass sie sich mit Problemen im Zusammenhang mit Zugangsdaten beschäftigen müssen

78% der **IT-Führungskräfte** sagen, dass ihre Teams sich mindestens wöchentlich mit Passwortproblemen von Mitarbeitende beschäftigen

28 % der **IT-Führungskräfte** sagen, dass Passwortprobleme täglich oder sogar mehrmals am Tag auftreten

---

„Burnout unter IT-Führungskräften ist seit Jahren ein Problem“, sagt Rivain. „Dieses Problem wird sich mit der Bedrohung durch

KI-gestützte Phishing-Angriffe nur noch verschlimmern.“

Fazit

Neue Lösungen für neue Herausforderungen

Versetzen Sie IT-Teams in die Lage, Bedrohungen für Zugangsdaten zu erkennen und darauf zu reagieren

Auf dem Weg in eine passwortlose Zukunft ist die nächste Entwicklungsstufe zum Schutz von Zugangsdaten und zur Unterstützung die proaktive Sicherheit von Zugangsdaten, die potenzielle Schwachstellen offenbart und Administratoren vor riskantem Verhalten warnt – ohne dass zusätzliche Mitarbeitende oder Ressourcen erforderlich sind.

Mit diesem Ansatz erhalten IT-Teams umsetzbare Daten in Echtzeit, damit sie:

- Versteckte Bedrohungen wie Schatten-IT und riskantes menschliches Verhalten erkennen können, das auf schlechte Passworthygiene zurückzuführen ist
- Automatisch auf Bedrohungen mit kontextbezogenen, momentanen Aufforderungen und Schulungen reagieren können
- Ihr Unternehmen mit einer Lösung schützen können, der sie vertrauen können und die Mitarbeitende annehmen

Die Sicherheit von Zugangsdaten hat einen Wendepunkt erreicht. Klar ist, dass die einfache Verwaltung von Zugangsdaten nicht mehr ausreicht –

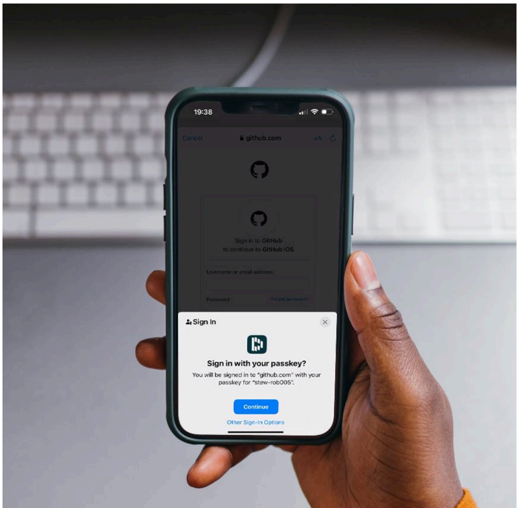
„Eine gute Passworthygiene kommt nicht von alleine“, sagt Dashlane-Kunde Abhilash Rajan, Senior Director of

Technology, Systems, and Facility Operations bei New America. „Man braucht die richtigen Tools zur Unterstützung.“

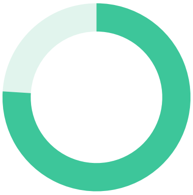
die heutigen Herausforderungen erfordern neue Lösungen. Für IT-Führungskräfte, die in Echtzeit erfahren möchten, wenn jemand im Unternehmen im Zusammenhang mit Zugangsdaten ein riskantes Verhalten an den Tag legt, und die eigenen Teams in die Lage versetzen möchten, schnell zu handeln, ist eine proaktive Verwaltung von Zugangsdaten eine Chance ein echter Paradigmenwechsel.

Passwortlos: Der Schlüssel zum Aufbau eines Phishing-resistenten Unternehmens

Das Passwort ist der Kern vieler Risiken, denen Unternehmen ausgesetzt sind. Auch Administratoren und Mitarbeitenden empfinden es als Last. Seit seiner Erfindung vor mehr als 50 Jahren zum Schutz eines Großrechners erfunden wurde, dient das Passwort aufgrund seiner Anfälligkeit für Social-Engineering- und Malware zum Diebstahl von Zugangsdaten mehr schlecht als recht als Sicherheitskontrolle.



Unternehmen überlegen jetzt ernsthaft, was nach dem Passwort kommt. Unseren Berichtsergebnissen zufolge sagen 61 % der IT-Führungskräfte, dass ihr Unternehmen irgendwann passwortlos sein wird. 16 % der Unternehmen implementieren bereits jetzt irgendeine Form von passwortloser Authentifizierung. Am vielversprechendsten,



76 %

der **IT-Führungskräfte** sagen, dass die Vorstandsebene auf die Einführung von Passkeys drängt,

was zeigt, wie passwortlose Verwendung durch Verbraucher in den Führungsetagen der Unternehmen ankommt.

Trotz des Versprechens einer sichereren und einfacheren passwortlosen Zukunft werden Unternehmen aufgrund der Komplexität von Unternehmensumgebungen möglicherweise nie vollständig auf Passwörter. verzichten können Die Notwendigkeit eines

umfassenden, mehrschichtigen Ansatzes zur Minderung von Risiken bei Zugangsdaten ist zwingend erforderlich.

> „Es ist leicht, Mitarbeitenden die Schuld zu geben, wenn etwas passiert“, sagt Rivain. „Aber liegt es eigentlich nicht eher an der schlechten Technologie, die Mitarbeitende überhaupt Risiken aussetzt?“

Copyright © 2025 Dashlane

Lernen Sie die proaktive Sicherheitsplattform für Zugangsdaten von Dashlane kennen und erfahren Sie, wie unsere Lösung dazu beitragen kann, die Herausforderungen Ihres Unternehmens im Hinblick auf die Sicherheit von Zugangsdaten und die Risiken für Menschen in den Griff zu bekommen.

Über Dashlane

Dashlane ist die führende Sicherheitsplattform für Zugangsdaten, die den Zugriff sichert und proaktiv vor Sicherheitsverletzungen schützt. Über 24.000 Marken weltweit, einschließlich Air France, Forrester Research und Sephora, vertrauen Dashlane und dessen branchenführenden Innovationen, um der Konkurrenz mit Blick auf neue Bedrohungen einen Schritt vorauszubleiben. Das Unternehmen kombiniert patentierte, Sicherheit der Enterprise-Klasse mit verbraucherfreundlichem Design in einer erstklassigen Plattform, damit alle Teil der Sicherheitslösung für Zugangsdaten sein können.

Besuchen Sie dashlane.com/de/blog, um weitere Ressourcen, Tipps für digitale Sicherheit und Produktneuheiten von Dashlane zu erhalten.

DASHLANE

Besuchen Sie dashlane.com