LastPass by LogMeIn

10 Tipps
für optimale Sicherheit und Produktivität im Homeoffice

Homeoffice bietet Unternehmen viele Vorteile, hat aber auch ihre Tücken:

- Wie steht es dabei um die Sicherheit des Unternehmens?
- Wie können Homeoffice-Mitarbeiter auf ihre Arbeitsressourcen zugreifen?

Tipp 1 Single Sign-On

Dank Single Sign-On kann Ihre IT zentral den Zugriff verwalten und Zugriffsrechte vergeben und entziehen.

90 % **halten die Verwaltung des Benutzerzugriffs im Hinblick auf die Unternehmenssicherheit für wichtig.[1]**

Tipp 2 Multifaktor-Authentifizierung

Mit MFA führen Sie eine weitere Sicherheitsebene ein. Biometriefunktionen sorgen dabei für eine nahtlose Anmeldung.

59 % **halten eine stärkere Benutzerauthentifizierung für entscheidend bei der Identitäts- und Zugriffsverwaltung (IAM).[1]**

Tipp 3 Kontextabhängige Faktoren

Kontextuelle Richtlinien passen Authentifizierungsanforderungen an die jeweilige Situation an und verbessern so Flexibilität und Kontrolle.

60 % **sind der Meinung, dass MFA für eine bessere Unternehmenssicherheit sorgt.[1]**

Tipp 4 VPN-Sperre

Mit starken Passwörtern und MFA für Ihr VPN stellen Sie sicher, dass Ihre Mitarbeiter vor dem Zugriff darauf ihre Identität bestätigen.

80 % **aller Datenschutzverletzungen sind auf schwache, wiederverwendete oder gestohlene Passwörter zurückzuführen.[2]**

Tipp 5

Workstation-Schutz

Mit MFA können sich nur rechtmäßige Benutzer auf Workstations anmelden – auch wenn diese kompromittiert sind.

30 %

der Datenschutzverletzungen betreffen Workstations.[2]

Tipp 6

Sichere Freigabe

Mit einer Passwortfreigabefunktion können Mitarbeiter Anmeldedaten mit Kollegen teilen, sodass alle auf die erforderlichen Arbeitsressourcen zugreifen können.

185

freigegebene Ordner sind im Schnitt pro Unternehmen in Gebrauch.[3]

Tipp 7 Weniger Passwörter

Eine passwortfreie Authentifizierung erspart die Passworteingabe bei der Systemanmeldung und gibt effizienten und sicheren Zugriff auf Arbeitsressourcen.

95 % **der IT-Sicherheitsexperten sind der Meinung, dass ihr Unternehmen mehr Wert auf hohe Passwortqualität legen sollte.[1]**

Tipp 8 Schatten-IT im Griff

Ein Passwort-Manager garantiert sichere Verwahrung für alle Anmeldedaten – die der IT bekannten sowie die, von denen sie nichts weiß.

77 % **der Mitarbeiter nutzen externe Cloud-Anwendungen ohne die Zustimmung oder das Wissen der IT-Abteilung.[4]**

Tipp 9 Schutz vor Phishing

Passwortverwaltung unterbindet die automatische Eingabe von Passwörtern auf verdächtigen Websites und senkt so das Risiko von Phishing.

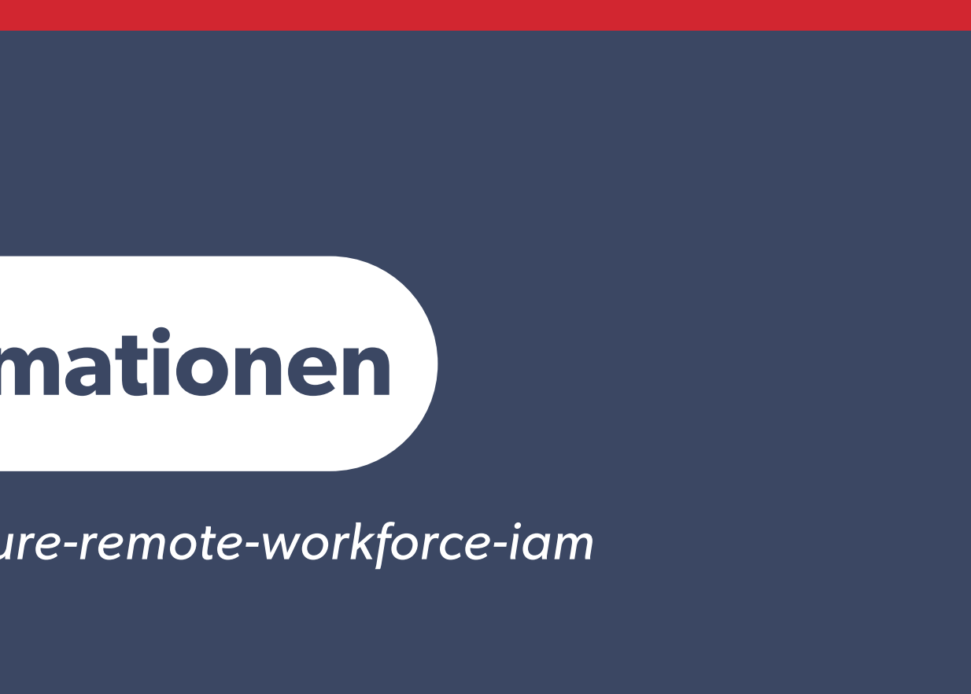
26,5 % der Empfänger verdächtiger E-Mails klicken auf die darin befindlichen Links.[5]

Tipp 10 Umfassender Überblick

Mithilfe ausgefeilter Berichte überwachen Sie die Aktivität bei Zugriff und Authentifizierung und können beides bedarfsgerecht anpassen.

53 % **halten die Überwachung der Benutzeraktivität für eine wichtige IAM-Funktion.[1]**

Homeoffice, einfach und sicher mit IAM



Mit der richtigen IAM-Strategie ist Homeoffice kein Problem.

Produktives Arbeiten für Ihr Personal im Homeoffice, Schutz für Ihr Unternehmen und die Ressourcen: LastPass Identity ermöglicht beides. Informieren Sie sich.

Weitere Informationen

www.lastpass.com/solutions/secure-remote-workforce-iam

Quellen:

1 Der Leitfaden für moderne Identitätsverwaltung
2 2019 Verizon Data Breach Investigations Report
3 LastPass State of the Password Report 2019
4 NTT Com, Shadow IT Survey, 2016
5 IBM State of the Phish Research 2019

03.31.2020/PDF/LMI1356