IDC INFOBRIEF ZEIGT: SO MACHT IT-SECURITY UNTERNEHMEN ZUKUNFTSFÄHIG

Hier mehr erfahren

Im „New Normal" hat sich die Wahrnehmung von IT-Sicherheit im Unternehmen massiv verändert. Ein LastPass/ IDC Infobrief zeigt, wie IT in Unternehmen Zukunft ermöglicht.

Sicherheit für Remote-Arbeit und trotzdem ein nahtloses Nutzererlebnis

Im „New Normal" und mit Remote Work hat sich jetzt schon vieles geändert. Ganz vorne mit dabei: die Wahrnehmung von IT-Sicherheit im Unternehmen, die sich als extrem hilfreich erwiesen hat, die richtigen Bedingungen für diese neue Art von Zusammenarbeit zu gewährleisten.

Schlüsselrolle für Identity und Access Management

IDC hat dazu in Zusammenarbeit mit LastPass ein ausführliches Infobrief-Paper erarbeitet. Die Argumentationskette liegt auf der Hand: Modernes Identity und Access Management ermöglichen komfortables, nahtloses und effizientes Arbeiten mit unterschiedlichen Geräten von verschiedenen Orten aus, ohne dabei die hohen Sicherheitsanforderungen von Unternehmen zu verraten. Identity und Access Management, der Einsatz eines Passwortmanagers: Das sind Maßnahmen, die den Anforderungen aller Stakeholder gerecht werden. IT-Security schafft es so, den neuen Sicherheitsanforderungen für Remote-Arbeit Rechnung zu tragen und trotzdem für ein gutes, nahtloses Nutzererlebnis zu sorgen.

Generell raten die Sicherheitsexperten von LastPass, die folgenden Schritte in Erwägung zu ziehen:

1 Single Sign-on einsetzen

SSO verschafft der IT übersichtlich die volle Kontrolle und vereinfacht die Verwaltung von Access. Ein nahtloses Nutzungserlebnis für User, ohne in der IT auf Transparenz und Kontrolle über Benutzerzugriff zu verzichten.

2 Multifaktor-Authentifizierung einführen

MFA schafft eine zusätzliche Sicherheitslinie für das Unternehmen und den Usern durch den Einsatz biometrischer Daten ein angenehmes Nutzungserlebnis wie etwa passwortfreies Anmelden (übrigens: 60 Prozent der MFA-Nutzer finden, dass MFA mehr Sicherheit in die Organisation gebracht hat).

3 Kontextfaktoren nutzen

Der Einsatz von Kontextfaktoren wie Lokalisierung oder IP-Adressen verschafft der IT zusätzliche Kontrolle und Sicherheit, indem simpel und einfach die Plausibilität der Anmeldesituation mit berücksichtigt wird (Zeitpunkt, Ort, Device).

4 VPN sichern

Starke Passwörter und MFA auf dem VPN stellen sicher, dass Ihre sich anmeldenden Mitarbeiter auch wirklich die sind, die sie zu sein behaupten – und zwar, bevor sie Access erhalten.

5 Workstations schützen

MFA auf Workstations sorgt dafür, dass sich nur legitimierte Personen authentifizieren können (etwa durch die Verwendung biometrischer und kontextueller Faktoren).

6 Sicher teilen

Password Sharing stellt sicher, dass jeder Zugang zu den Daten hat, die er zum Arbeiten benötigt.

7 Passwörter reduzieren

Passwortfreie Authentifizierung lässt das Passwort aus dem Log-in-Prozess verschwinden und sorgt für ein nahtloses Nutzungserlebnis.

8 „Shadow IT" anpacken

Ein Passwortmanager bietet Mitarbeitern einen sicheren Ort für Zugangsdaten – ob die IT davon weiß oder nicht.

9 Phishing-Muster verhindern

Passwort-Management kann helfen, das Risiko von Phishing zu mildern, indem es niemals Aktionen auf verdächtigen Seiten ausführt.

10 Den Überblick behalten

Detaillierte Reports verschaffen den Überblick über alle Aktivitäten und ermöglichen Anpassungen bei Access und Authentifizierung – dort, wo es notwendig ist.

Eine veränderte Wahrnehmung von IT-Security

Dass sich IT-Security in diesem Zusammenhang auch gegenüber dem Management besser positionieren kann, ist mehr als nur ein Nebeneffekt. IAM wird helfen, die Rolle von IT langfristig zu stärken – ein Umstand, der allen Beteiligten zugutekommen wird. Das ist auf jeden Fall einen Blick wert. Schauen Sie sich die Studie an.

Barry McMahon, Senior Manager IAM, LastPass by LogMeIn

LastPass by LogMeIn