

# Finanzen: Risikominderung und integrierte IAM-Infrastruktur



Finanzdienstleister haben Umgang mit etwas, das datentechnisch höchst sensibel ist: Geld. Die Risiken in dieser Branche sind besonders hoch, was Konsequenzen für den Umgang mit dem Zugriff und der Authentifizierung von Mitarbeitern hat.

## Risikominderung ist sehr wichtig.

**70 % Finanzunternehmen**

**66 % Alle Unternehmen**



Aufgrund der hohen Sensibilität ihrer Daten ist die Finanzbranche stark reguliert und hat international zahlreiche Gremien, Gesetze und Richtlinien hervorgebracht, z. B. **die Financial Action Task Force (FATF), den Bank Secrecy Act (BSA) oder die EU-Geldwäscherichtlinie 5AMLD.** Im Kontext von IAM hat Risikominderung hier eine höhere Priorität als in anderen Branchen.

## Unser Unternehmen war bereits Opfer eines Hackerangriffs.

**35 % Finanzunternehmen**

**31 % Alle Unternehmen**



Im Hinblick auf Cyberangriffe hat die Branche noch einiges nachzuholen. Finanzdienstleister und ihre Kunden sind schon lange im Visier krimineller Hacker und haben mit 18,3 Millionen US-Dollar jährlich **die von allen Branchen höchsten Kosten im Zusammenhang mit Cyberangriffen.**<sup>1</sup>

## Als Erstes möchten wir die Integration der Sicherheitsinfrastruktur verbessern.

**65 % Finanzunternehmen**

**57 % Alle Unternehmen**



**Priorität hat bei Finanzunternehmen das Thema Integration.** Integrationen geben umfassenden Überblick über Benutzerzugriff und die Authentifizierung und wappnen das Unternehmen besser gegen die zunehmenden Hackerangriffe.

## Wir haben nicht genügend Budget für IAM.

**17 % Finanzunternehmen**

**24 % Alle Unternehmen**



Budgetknappheit ist in der Finanzbranche weniger Thema. **Die Branche kennt ihre Risiken** und investiert 14 % ihres IT-Jahresbudgets in Cybersicherheitsprogramme.<sup>2</sup>

## Wir haben bereits in MFA investiert.

**55 % Finanzunternehmen**

**48 % Alle Unternehmen**



Im Investitionsbudget wird **MFA der erste Rang eingeräumt.** Dies verdankt sich höchstwahrscheinlich der Empfehlung des US-amerikanischen National Institute of Standards and Technology (NIST), den Zugriff auf Systeme durch MFA sicherer zu machen.

## Wir planen die Investition in eine Passwortverwaltung.

**32 % Finanzunternehmen**

**22 % Alle Unternehmen**



In der Finanzbranche spielt **Passwortverwaltung eine deutlich stärkere Rolle als in anderen Branchen.** Dies könnte daran liegen, dass der Umgang mit sensiblen Zugangsdaten hier zum Arbeitsalltag gehört. Passwortverwaltung ermöglicht die sichere Verwaltung und Freigabe von Zugangsdaten – und trägt dadurch zur angestrebten Risikominderung bei.

## Wir brauchen ein integriertes System zur Verwaltung, Überwachung und Einrichtung von Richtlinien.

**58 % Finanzunternehmen**

**44 % Alle Unternehmen**



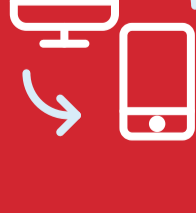
Für Finanzunternehmen ideal ist eine IAM-Lösung, **die eine integrierte Handhabung von Benutzerzugriff und Authentifizierung ermöglicht,** was den Integrationsprioritäten der Branche entspricht. Die unternehmensweite IAM-Verwaltung wird durch Integrationen einfacher.

## UNSERE EMPFEHLUNGEN FÜR DIE FINANZBRANCHE



### Führen Sie flächendeckend MFA ein.

Mit MFA für Anwendungen, Workstations von Mitarbeitern und das VPN lassen sich Risiken auf einfache Weise mindern und Compliance-Vorgaben und Audits leichter bewältigen.



### Achten Sie auf Integrationen und Flexibilität.

Ideal sind IAM-Lösungen, die eine Vielzahl von Integrationen bieten und ein Arbeiten mit Ihren bevorzugten Tools gestatten.



### Führen Sie ein zentrales IAM ein.

Eine einheitliche Sicht auf den Zugriff und die Authentifizierung von Mitarbeitern beugt Risiken vor.

Weitere Informationen finden Sie unter:  
<https://www.lastpass.com/de/products/identity>.