



IM FOKUS:
IT IM
FINANZSEKTOR

IT-Administration im Finanzsektor: Trends und Handlungsfelder

Trend Guide

Komplexität als New Normal

Der Finanzsektor steht unter permanentem Innovationsdruck – und muss gleichzeitig immer vielfältigere IT-Umgebungen managen. Hybride Arbeitsmodelle, KI-Tools und mobile Endgeräte treffen auf jahrzehntealte zentrale Bankinfrastruktur und Geldautomaten. Von IT-Teams wird erwartet, diese heterogene Landschaft sicher, effizient und regulatorisch konform zu betreiben.

Dieser Bericht liefert Zahlen, Trends und Empfehlungen für den Wechsel von reaktiver Problemlösung zu proaktiver Innovation. Die folgenden Themen stehen im Fokus:



**Hybrides
Arbeiten und
BYOD**



**Cybersicherheits-
risiken an
Endpunkten**



**Regulatorische
Anforderungen**



**Der Aufstieg von
UEM
und DEX-Tools**

Hybrides Arbeiten und IT-Fragmentierung

Seit der Pandemie 2020 hat sich die Arbeitskultur im Finanzsektor nachhaltig verändert. Hybride Modelle sind Standard: Außendienst, Filialteams und Zentrale arbeiten standortübergreifend. Für die IT bedeutet das: eine rasant wachsende Vielfalt an Endgeräten, Betriebssystemen und Netzwerken zu managen – vor Ort, mobil und im Homeoffice.

Der BFSI Digital Operations Brief 2023 von Forrester zeigt: Banken, die schnell auf Hybrid-Computing umgestellt haben, verzeichneten einen 40 %-Anstieg an Endgerät-bezogenen IT-Tickets – vor allem, wenn Monitoring- und Automatisierungslösungen fehlten.



der IT-Teams unterstützen hybride oder vollständig remote Arbeitsmodelle (IDC, 2023)



der täglichen Arbeit läuft über Cloud- oder Web-Anwendungen (Forrester, 2023)



der Mitarbeitenden im Finanzsektor berichten von höherer Produktivität durch hybride Modelle (Kyndryl, 2023)

Auswirkungen

- Erhöhter Bedarf an zentralem Gerätemanagement
- Mehr Komplexität durch unterschiedliche Hardware und Betriebssysteme
- Erfordert einheitliche Sicherheits- und Update-Strategien für alle Endgeräte

Bring Your Own Device (BYOD) ist im BFSI-Sektor längst etabliert. Besonders in Bereichen wie Kundenbetreuung, Außendienst oder Vertrieb setzen Mitarbeitende vermehrt auf ihre privaten Mobilgeräte. Das steigert Flexibilität und Effizienz – birgt aber auch erhebliche Sicherheitsrisiken, wenn keine klaren Regeln gelten.

Laut der ISACA-Banksicherheitsstudie 2023 bewerten 52 % der mittelgroßen Banken in der EU BYOD als größte Lücke in ihrer Endpunktsicherheit – und als zentrales Thema in internen Audits, insbesondere im Hinblick auf Geschäftskontinuität und Betrugsprävention.



- › Produktivitätssteigerungen von bis zu 68 % bei mobilem Zugriff (Bitglass, 2022)
- › Einsparungen von 250–350 USD pro Mitarbeitendem und Jahr (Gartner, 2023)
- › Mehr als 75 % der Mitarbeitenden nutzen gelegentlich private Geräte für berufliche Zwecke (ENISA, 2023)



- › 32 % der Unternehmen haben keine formelle BYOD-Registrierung (ENISA, 2023)
- › 17% der Nutzenden greifen ohne Wissen der IT-Abteilung auf Unternehmensdaten zu (IDC, 2023)
- › Fehlende Transparenz erhöht Sicherheits- und Compliance-Risiken

LÖSUNG UEM-Plattformen ermöglichen es:

- › private Geräte sicher zu registrieren und zu überwachen
- › Verschlüsselung und App-Richtlinien durchzusetzen
- › Geräte bei Bedarf aus der Ferne zu sperren oder zu löschen

Cybersicherheitsrisiken: Endgeräte als Hauptangriffsfläche

Der Regional Cyber Resilience Report 2023 (FS-ISAC) zeigt: Für mittelständische BFSI-Unternehmen sind kompromittierte Endpunkte inzwischen die Hauptursache für Betrugsverluste – noch vor Phishing oder Credential-Diebstahl. Damit wird Endpoint Security zur zentralen Kontrollinstanz in der Betrugsprävention.

Endpunkte sind nach wie vor der bevorzugte Angriffsvektor. Phishing, Ransomware und Insider-Bedrohungen richten sich direkt gegen die Geräte der Mitarbeitenden.



der EU-Banken und 17 % der Versicherer waren 2023 von Ransomware betroffen (ENISA, 2023)



der Finanzunternehmen verschlüsseln gespeicherte Daten auf Endgeräten immer noch nicht (Jones Walker 2024)



der kritischen Schwachstellen werden innerhalb von 30 Tagen geschlossen (Qualys 2023)

4

der fünf größten KI-Risiken im Finanzsektor betreffen Datenschutz und Datensicherheit (FCA), 2025)

INVESTITIONSTRENDS

- › Cybersicherheit beansprucht inzwischen **9–10 %** des gesamten IT-Budgets
- › Endpoint Protection Lösungen sind Standard, vielen mittelständischen Unternehmen fehlen jedoch erweiterte EDR/XDR-Systeme



PRIORITÄTEN

- › Vollständige Festplattenverschlüsselung mit sicherem Schlüsselmanagement
- › Automatisiertes und zeitnahes Patch-Management
- › Moderne Erkennungstechniken gegen Malware und verdächtiges Verhalten
- › Regelmäßige Schwachstellenscans mit konkreten Handlungsempfehlungen
- › KI-basierte Sicherheitslösungen mit integriertem Datenschutz

Regulatorischer Druck treibt die Modernisierung

Regulierungsbehörden in der EU und den USA verschärfen ihre Anforderungen. Compliance bedeutet heute nachweisbare Umsetzung, nicht nur Dokumentation.

EU-VORGABEN



- › **NIS2 Directive (2024):** stärkt Sicherheit und Resilienz in kritischen Sektoren, einschließlich BFSI
- › **DORA (2025):** fordert umfassendes IKT-Risikomanagement mit Fokus auf Endpunkte, Verschlüsselung und Incident Response

US-VORGABEN



- › **FFIEC:** verlangt risikobasierte Endpunkt-Kontrollen
- › **GLBA and SEC:** verpflichten zu strikter Cyberhygiene und Incident Reporting

Der Financial Services Compliance Outlook 2023 (Capgemini) zeigt:

- 71 % der EU-Finanzunternehmen überprüfen oder überarbeiten aufgrund von DORA ihre Endpunktsicherheitsrichtlinien
- 62 % der mittelgroßen US-Banken haben mit GLBA-bedingten Compliance-Lückenanalysen begonnen

Compliance verschiebt sich damit von der Dokumentation zur Umsetzung. Aufsichtsbehörden erwarten überprüfbare Sicherheitsresultate – nicht nur Richtlinien.

Transparenz
über alle End-
punkte

Klare Richt-
liniendurch-
setzung (z. B.
Passwörter,
Fernlöschung)

Zentrale Proto-
kollierung und
automatisierte
Warnmel-
dungen

Compliance-
Validierung mit
revisionssiche-
rer Dokumenta-
tion

Vom Kontrollfokus zur Nutzererfahrung: Der Aufstieg

Laut BCG Banking Workforce Benchmarking Report 2023 erzielen Banken mit DEX-Initiativen doppelt so hohe Mitarbeiterzufriedenheit im Außendienst und Kundenservice sowie 23 % niedrigere interne Supportkosten

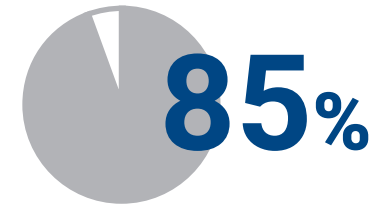
Digital Employee Experience (DEX)-Plattformen verbinden Endpunkt-Management mit Produktivität. Gerade im Finanzsektor, wo Vertrauen und Verfügbarkeit geschäftskritisch sind, reduzieren sie Ausfallzeiten und Kosten.



der BFSI-Unternehmen setzen DEX-Tools ein (Forrester, 2023)



der Teams widmen 10 bis 20 Stunden/Woche dem proaktiven Support für Endbenutzer (Auvik, 2024)



der Versicherer priorisieren ESG in Kernfunktionen (PWC, 2023)



der BFSI-Organisationen werden DEX-Kennzahlen nun an CIOs gemeldet (Gartner, 2023)

Warum DEX wichtig ist

- Probleme werden gelöst, bevor Support-Tickets entstehen
- DEX-Daten unterstützen Budgetplanung, Toolauswahl und Lieferantensteuerung
- Mitarbeitererfahrung ist direkt mit Geschäftsergebnissen verknüpft
- Längere Gerätelebensdauer senkt Kosten und CO2-Fußabdruck

IT-Führungskräfte im Finanzsektor sind heute nicht mehr nur Systemverwalter, sondern Gestalter von Innovation, Sicherheit und Compliance. Der Schlüssel liegt darin, Komplexität aktiv zu steuern und die IT auf Zukunftsfähigkeit auszurichten.

Komplexität wird so zur Klarheit – und Legacy-Systeme zum Fundament für nachhaltige Wettbewerbsstärke.

Sie möchten mehr erfahren?



Hier beginnt Ihr Weg zu einer sicheren und effizienten IT-Infrastruktur.

Checkliste für Entscheider

- ✓ UEM-Plattform zur Tool-Konsolidierung einführen
- ✓ Endpunkte konsequent absichern (verschlüsseln, patchen, schützen)
- ✓ BYOD- und Mobile-Sicherheitsrichtlinien klar regeln
- ✓ DEX-Tools zur Prozess- und Serviceoptimierung nutzen
- ✓ IT-Kontrollen an regulatorische Rahmenwerke anpassen

Kontakt

 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Deutschland

 + 43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA



baramundi software

baramundi entwickelt Unified-Endpoint-Management-Lösungen für die zentrale Verwaltung von PCs, mobilen Geräten und Servern. Die Software automatisiert die Verteilung von Anwendungen, vereinfacht das Patch-Management und sorgt für Transparenz im Netzwerk. Damit leisten baramundi-Lösungen einen wichtigen Beitrag zur IT-Sicherheit und zur optimalen Nutzung von IT-Ressourcen.

www.baramundi.com