WHITEPAPER

DORA-Compliance und Privileged Access Management (PAM)

segura®

Futureproof
Identity Security

www.
segura.
security

Wie Finanzinstitute ihren DORA-Reifegrad mit PAM stärken können

Finanzinstitute sind auf digitale Systeme, Drittanbieter, Cloud-Umgebungen, Remote-Zugriffe, privilegierte User, Maschinenidentitäten, Secrets und Zertifikate angewiesen, um geschäftskritische Prozesse aufrechtzuerhalten.

Diese Abhängigkeit führt zu operativen Risiken, da kompromittierte Zugangsdaten, nicht verwaltete Adminkonten, abgelaufene Zertifikate oder unüberwachte Sitzungen externer Dienstleister verschiedene Services beeinträchtigen, Wiederherstellungsmaßnahmen verzögern und Audits oder Untersuchungen erschweren.

Mit dem **Digital Operational Resilience Act (kurz: DORA)** hat die Europäische Union einen Rechtsrahmen geschaffen, um die digitale operationelle Resilienz im Finanzsektor zu stärken. DORA gilt dabei für Finanzunternehmen sowie für bestimmte IKT-Drittdienstleister. Die Verordnung ist seit dem 17. Januar 2025 verbindlich anzuwenden und verpflichtet dazu, IKT-bezogene Störungen zu verhindern, ihnen standzuhalten, entsprechend darauf zu reagieren und sich davon zu erholen. Dazu zählen Cyberangriffe, Systemausfälle, Serviceunterbrechungen und technologiebezogene Vorfälle bei Drittanbietern.

Für Finanzinstitute besteht die zentrale Herausforderung darin, nachzuweisen, dass kritische Systeme wirksam gesteuert, überwacht, getestet, geschützt und wiederherstellbar sind.

Privilegierte Zugriffe bieten dabei eine der naheliegendsten Ansatzpunkte.

DORA schreibt keine bestimmte Privileged-Access-Management-Lösung vor. Viele DORA-Anforderungen setzen jedoch eine wirksame Kontrolle über Identitäten, Zugangsdaten, privilegierte Zugriffe, Zugriffe von Drittanbietern sowie Monitoring, Protokollierung und Audit-Nachweise voraus.

Was deckt DORA ab?

DORA wird üblicherweise anhand von sechs zentralen Anforderungsbereichen beschrieben. Für Security- und IT-Teams laufen diese Anforderungen häufig auf eine zentrale Herausforderung hinaus: den Nachweis, dass Zugriffe auf kritische Systeme **vor, während** und **nach** Störungen kontrolliert werden.

1. IKT-Risikomanagement

Finanzunternehmen müssen ein IKT-Risikomanagement-Framework etablieren und betreiben, das Identifikation, Schutz, Erkennung, Reaktion und Wiederherstellung unterstützt.

Aus Sicht der Zugriffskontrolle bedeutet das, Transparenz darüber zu schaffen, wer Zugriff auf kritische Systeme besitzt, welche Konten erweiterte Berechtigungen haben, wo Zugangsdaten gespeichert werden und ob diese Zugriffe auf geschäftlich erforderliche Zwecke beschränkt sind.

2. IKT-Vorfallmanagement und Meldepflichten

DORA verpflichtet Finanzunternehmen dazu, schwerwiegende IKT-Vorfälle zu erkennen, zu klassifizieren, zu steuern und zu melden.

Im Fall eines Vorfalls sind belastbare Nachweise erforderlich. IT-Teams müssen nachvollziehen können, wer auf das betroffene System zugegriffen hat, welche Aktivitäten durchgeführt wurden, wann diese stattgefunden haben und ob der Zugriff genehmigt war.

3. Tests der digitalen operationellen Resilienz

Organisationen müssen die Wirksamkeit ihrer Resilienzmaßnahmen regelmäßig überprüfen und testen. Für Unternehmen mit erhöhtem Risikoprofil kann dies auch fortgeschrittene Testverfahren wie Threat-Led Penetration Testing (TLPT) umfassen.

Kontrollen für privilegierte Zugriffe sollten dabei Bestandteil dieser Tests sein. Dabei muss überprüft werden, ob Zugangsdaten geschützt sind, Adminzugriffe begrenzt, Sitzungen externer Dienstleister überwacht und Zugriffsrechte bei Bedarf entzogen werden können.

4. IKT-Drittparteienrisikomanagement

DORA betrachtet Technologierisiken von Drittanbietern als zentralen Bestandteil der operationellen Resilienz. Die Auslagerung von Services entbindet Finanzunternehmen daher nicht von ihrer Verantwortung.

Sie müssen kontrollieren, wie Anbieter, Dienstleister, Auftragnehmer und externe Administratoren auf kritische Systeme zugreifen. Diese Zugriffe sollten dann genehmigt, begrenzt, überwacht und wieder entzogen werden, sobald diese nicht mehr benötigt werden.

5. Informationsaustausch

DORA fördert den vertrauenswürdigen Austausch von Informationen zu Cyberbedrohungen, um Prävention, Erkennung und Reaktionsfähigkeit zu verbessern.

Verlässliche Zugriffsprotokolle helfen dabei, Vorfälle besser nachzuvollziehen und bei Bedarf präzisere Meldungen zu erstellen.

6. Aufsicht über kritische IKT-Drittdienstleister

DORA führt außerdem eine Aufsicht auf EU-Ebene für kritische IKT-Drittdienstleister ein, die den Finanzsektor unterstützen.

Für Finanzunternehmen unterstreicht dies die Notwendigkeit, nicht nur Vertragsbeziehungen zu verstehen, sondern auch Zugriffe von Dienstleistern, Abhängigkeiten, Zugangsdaten, Verantwortlichkeiten und Nachweispflichten im Blick zu behalten.

Warum privilegierte Zugriffe für DORA entscheidend sind

Privilegierte Zugriffe ermöglichen Usern, Admins, Anwendungen, Maschinenidentitäten und Drittanbietern den Zugriff auf sensible Systeme, die Verwaltung kritischer Infrastrukturen sowie die Durchführung von Änderungen und Maßnahmen im Rahmen von Sicherheitsvorfällen. Diese Zugriffe sind für den Geschäftsbetrieb unverzichtbar, lassen sich ohne geeignete Kontrollen jedoch nur schwer nachvollziehen.

Im Rahmen von Audits, regulatorischen Prüfungen oder Sicherheitsuntersuchungen müssen folgende Fragen beantwortet werden können:

- Wer verfügte über privilegierte Zugriffsrechte?
- Aus welchem Grund wurde der Zugriff gewährt?
- Wurde der Zugriff genehmigt?
- War der Zugriff zeitlich, rollenbasiert oder systemseitig eingeschränkt?
- Wurde die Sitzung überwacht?
- Welche Aktivitäten wurden durchgeführt?
- Wurden die Berechtigungen anschließend wieder entzogen?
- Können die erforderlichen Nachweise kurzfristig bereitgestellt werden?

Fehlt eine zentrale Dokumentation privilegierter Zugriffe, müssen relevante Informationen häufig manuell aus Log-Dateien, Ticketsystemen, Screenshots, Tabellen und einzelnen Benutzerkonten rekonstruiert werden. **Privileged Access Management (PAM)** reduziert dieses Risiko, indem Kontrolle, Überwachung und prüfbare Nachweise für privilegierte Zugriffe zentral bereitgestellt werden.

Wie Segura® bei DORA unterstützt

Die **Segura® 360° Privilege Platform** unterstützt Finanzinstitute dabei, privilegierte Zugriffe über User, Admins, Drittanbieter, Maschinenidentitäten, Secrets, Zertifikate, Cloud-Umgebungen und kritische Systeme hinweg zu steuern und zu dokumentieren.

Für Finanzunternehmen bedeutet dies weniger Aufwand bei der Nachweisführung sowie mehr Kontrolle und Transparenz über privilegierte Zugriffe.

Privilegierte Zugriffe steuern

Mit **Segura® PAM Core** lässt sich steuern, wer auf kritische Systeme zugreifen darf, wann Zugriffe erlaubt sind und welche Berechtigungsstufen vergeben werden.

Zugriffe können dabei über Richtlinien, Genehmigungsprozesse, Workflows, zeitliche Begrenzungen und regelmäßige Überprüfungen gesteuert werden. Dadurch wird das Least-Privilege-Prinzip unterstützt, dauerhaft bestehende Berechtigungen werden reduziert und risikobehaftete Berechtigungskombinationen vermieden.

Der **Segura® Endpoint Privilege Manager** kontrolliert zusätzlich lokale Berechtigungen auf allen Endgeräten, während **Segura® Cloud Entitlements** privilegierte Zugriffe in Cloud-Umgebungen verwaltet.

Zugangsdaten schützen und Risiken gemeinsam genutzter Konten reduzieren

Privilegierte Zugangsdaten zählen zu den attraktivsten Angriffszielen. Werden sie in Tabellen, Skripten, Browser-Speichern oder nicht verwalteten Tools abgelegt, entstehen unnötige Sicherheitsrisiken.

Segura® schützt privilegierte Zugangsdaten durch zentrales Vaulting, regelmäßige Credential-Rotation, Zugriffsrichtlinien, MFA, Session-Kontrollen und Audit-Nachweise. Bei gemeinsam genutzten oder generischen Konten sorgt Segura® durch Access Brokering, Session Monitoring und Session Recording dafür, dass privilegierte Aktivitäten einzelnen Usern zugeordnet werden können. Dadurch wird nachvollziehbar, wer auf ein System zugegriffen hat und welche Aktivitäten durchgeführt wurden.

Darüber hinaus stellt **Segura® MySafe** einen persönlichen Unternehmens-Vault für Passwörter, Secrets und sensible Dateien bereit, der zentralen Richtlinien unterliegt.

Admin-, Notfall- und Drittanbieterzugriffe absichern

Admin-, Notfall- und Drittanbieterzugriffe sind für den Geschäftsbetrieb erforderlich und müssen streng kontrolliert werden.

Segura® unterstützt dabei, privilegierte Zugriffe über Genehmigungsprozesse, zeitliche Begrenzungen, Credential-Rotation und Session Recording zu vergeben, zu überwachen und wieder zu entziehen. Dadurch können IT-Teams bei Sicherheitsvorfällen oder Wartungsarbeiten schnell handeln, ohne die Kontrolle über privilegierte Zugriffe zu verlieren.

Für externe Zugriffe bietet **Segura® Domum Remote Access** einen sicheren und granularen Fernzugriff für Mitarbeiter und externe User, ohne Zugangsdaten offenzulegen oder auf nicht verwaltete Zugriffsmethoden angewiesen zu sein. Es lässt sich festlegen, wer eine Verbindung herstellen darf, auf welche Systeme zugegriffen werden kann, wann Zugriffe erlaubt sind und wie Sitzungen überwacht werden.

Incident Response und Audit-Nachweise unterstützen

Privilegierte Aktivitäten werden bei Sicherheitsvorfällen, Audits oder regulatorischen Prüfungen häufig zu wichtigen Nachweisen.

Segura® unterstützt dabei, diese Aktivitäten zu überwachen, Anomalien zu erkennen und risikobehaftete Aktionen durch richtlinienbasierte Kontrollen zu reduzieren.

Session Recordings, Befehlsprotokolle, Zugriffshistorien, Genehmigungs-Workflows und Berichte schaffen die erforderliche Transparenz für Audits, Untersuchungen und regulatorische Prüfungen.

Secrets, Zertifikate und Maschinenidentitäten verwalten

DORA beschränkt sich nicht auf menschliche User. Moderne Finanzumgebungen sind auf Servicekonten, Maschinenidentitäten, DevOps-Secrets, Zertifikate, kryptografische Schlüssel, APIs und automatisierte Workflows angewiesen.

Der **Segura® DevOps Secret Manager** schützt und verwaltet Maschinenidentitäten und Secrets über Entwicklungs- und Betriebsumgebungen hinweg.

Der **Segura® Certificate Manager** unterstützt das Management des gesamten Zertifikatslebenszyklus und automatisiert Verlängerungsprozesse. Dadurch lassen sich Ausfälle durch abgelaufene oder nicht verwaltete Zertifikate vermeiden.

Zugriffe mit Change- und Incident-Prozessen verknüpfen

Privilegierte Zugriffe erfolgen häufig im Rahmen von Wartungsarbeiten, Sicherheitsvorfällen, Notfallmaßnahmen oder Service Requests.

Segura® integriert sich in **ITSM-Plattformen**, um Ticketinformationen vor der Vergabe privilegierter Zugriffe zu validieren und eine nachvollziehbare Verbindung zwischen genehmigten Anfragen und privilegierten Aktivitäten herzustellen. Dadurch wird der Aufwand für die manuelle Nachweisführung reduziert.

DORA-Anforderungen und Segura® Funktionen

DORA-Anforderungsbereich	Nachweispflicht für Finanzunternehmen	Wie Segura® unterstützt
Least-Privilege-Prinzip (PoLP) (RTS Art. 21)	Zugriffsrechte auf IKT-Ressourcen werden auf Basis des geschäftlichen Bedarfs und mit den minimal erforderlichen Berechtigungen vergeben.	Segura® PAM Core unterstützt das Management des gesamten Lebenszyklus privilegierter Zugriffe. Der Endpoint Privilege Manager kontrolliert lokale Berechtigungen auf Endgeräten, während Cloud Entitlements privilegierte Zugriffe in Cloud-Umgebungen verwaltet.
Funktionstrennung (SoD) (RTS Art. 21)	Berechtigungen werden getrennt vergeben, um unberechtigte Zugriffe auf kritische Daten und risikobehaftete Berechtigungskombinationen zu vermeiden.	Segura® unterstützt richtlinienbasierte Workflows für Genehmigungen, Überprüfungen und den Entzug von Zugriffsrechten. Dadurch lassen sich Funktionstrennungen umsetzen und übermäßige Berechtigungen reduzieren.
Benutzerverantwortlichkeit und gemeinsam genutzte Konten (RTS Art. 21)	Die Nutzung gemeinsamer oder generischer Konten wird eingeschränkt und privilegierte Aktivitäten können einzelnen Usern zugeordnet werden.	Segura® PAM Core steuert privilegierte Zugriffe, überwacht Sitzungen in Echtzeit und zeichnet Aktivitäten auf, damit Aktionen einzelnen Usern zugeordnet werden können.
Individuelles Credential Management für privilegierte User (Art. 21)	Privilegierte User speichern und nutzen Zugangsdaten sicher und entsprechend den Unternehmensrichtlinien, ohne auf unsichere Speicherorte oder die gemeinsame Nutzung von Zugangsdaten angewiesen zu sein.	Segura® MySafe bietet einen persönlichen Unternehmens-Vault für Passwörter, Secrets und sensible Dateien mit zentral definierten Richtlinien, MFA und Audit-Nachweisen.

Management von Admin- und Notfallzugriffen (Art. 21)	Admin-, privilegierte, Notfall- und Ad-hoc-Zugriffe können über kontrollierte Prozesse vergeben, angepasst, überprüft und entzogen werden.	Segura® PAM Core unterstützt die Kontrolle privilegierter Zugriffe durch Genehmigungsprozesse, zeitliche Begrenzungen, Credential Management, Monitoring und Widerrufs-Workflows. Cloud Entitlements verwaltet privilegierte Zugriffe in Cloud-Umgebungen. MySafe unterstützt zudem die sichere Speicherung sensibler Zugangsdaten.
Starke Authentifizierung und Fernzugriff (RTS Art. 21)	Netzwerk- und privilegierte Zugriffe erfolgen über starke Authentifizierungsverfahren und kontrollierte Verbindungsmechanismen.	Segura® Domum Remote Access bietet einen sicheren und granularen Fernzugriff für Mitarbeiter und externe User, ohne Zugangsdaten offenzulegen oder auf nicht verwaltete Zugriffsmethoden angewiesen zu sein.
Anomalie- und Bedrohungserkennung (DORA Art. 10 / RTS Art. 23)	Organisationen können ungewöhnliche Aktivitäten, verdächtiges Verhalten bei privilegierten Zugriffen und potenzielle zugriffsbezogene Bedrohungen frühzeitig erkennen.	Segura® unterstützt dabei, privilegierte Aktivitäten zu überwachen, verdächtiges Verhalten und Anomalien zu erkennen sowie richtlinienbasierte Kontrollen durchzusetzen, um risikobehaftete Aktionen zu reduzieren.
Kryptografische Schlüssel, Secrets und Zertifikate (RTS Art. 6, Art. 7)	Kryptografische Schlüssel, Maschinenidentitäten, Secrets und digitale Zertifikate werden über ihren gesamten Lebenszyklus hinweg geschützt und verwaltet.	Der Segura® Certificate Manager unterstützt das Management des Zertifikatslebenszyklus und automatisiert Verlängerungsprozesse. Der Segura® DevOps Secret Manager schützt und verwaltet Maschinenidentitäten und Secrets über Entwicklungs- und Betriebsumgebungen hinweg.
Protokollierung und Audit Trails (RTS Art. 12)	Zugriffsbezogene Ereignisse werden protokolliert und überwacht, um Untersuchungen, Audits und die Erkennung von Anomalien zu unterstützen.	Segura® PAM Core zeichnet privilegierte Sitzungen, Befehle, Zugriffshistorien und die Nutzung von Zugangsdaten auf, um eine belastbare Audit-Trail-Dokumentation bereitzustellen.
IKT-Vorfallmanagement und Nachvollziehbarkeit von Änderungen (DORA Art. 17–23 / RTS Art. 17)	Privilegierte Zugriffe, die im Rahmen von Vorfällen, Wartungsarbeiten oder Änderungen gewährt werden, lassen sich genehmigten Geschäftsprozessen zuordnen.	Segura® integriert sich in ITSM-Plattformen, um Ticketinformationen vor der Vergabe privilegierter Zugriffe zu validieren und privilegierte Aktivitäten mit genehmigten Anfragen, Änderungen, Vorfällen oder Service-Tickets zu verknüpfen.

Fazit

DORA verpflichtet Finanzunternehmen dazu, IKT-Risiken zu steuern, Vorfälle zu melden, Resilienzmaßnahmen zu testen und die Wirksamkeit ihrer Kontrollen nachzuweisen.

Privileged Access Management (PAM) unterstützt diese Anforderungen durch die kontrollierte Verwaltung privilegierter Zugriffe auf kritische Systeme.

Mit der **Segura® 360° Privilege Platform** erhalten Sie mehr Kontrolle über privilegierte User, Zugangsdaten, Sessions, Maschinenidentitäten, Secrets, Zertifikate und Cloud-Umgebungen. Die Plattform unterstützt dabei, Zugriffsrisiken zu reduzieren und belastbare Audit-Nachweise bereitzustellen.

Wenn Sie sich auf DORA vorbereiten, sind privilegierte Zugriffe ein praxisrelevanter Startpunkt zur Stärkung Ihrer digitalen operationellen Resilienz.

Hinweis:
Dieses Whitepaper dient ausschließlich zu Informationszwecken und stellt keine rechtliche, regulatorische oder Compliance-Beratung dar. Die Anforderungen von DORA können je nach Unternehmensstruktur, angebotenen Services, regulatorischem Status, geografischer Ausrichtung und Beziehungen zu Drittanbietern unterschiedlich ausfallen. Konsultieren Sie Ihre Rechts-, Compliance- und Regulierungsverantwortlichen, um die konkrete Relevanz von DORA für Ihre Organisation zu bewerten.

Kontakt

Benötigen Sie einen belastbaren Nachweis privilegierter Zugriffe für DORA?
Wir unterstützen Sie dabei, Zugriffskontrolle, Monitoring und Audit-Nachweise zentral bereitzustellen.

Website:
www.segura.security

E-Mail::
dagma.dach@dagma.eu

Telefon:
+49 (0) 30 6920629-80

WHITEPAPER

DORA-Compliance und Privileged Access Management (PAM)