PROFI.info

SECRETS- & IDENTITY MANAGEMENT

WIE MODERNE UNTERNEHMEN SICHERHEIT, COMPLIANCE UND AGILITÄT VEREINEN

PROFI
Wir entwickeln mehr als IT

Kapitel 1: Das Problem: Credentials sind überall – und das ist gefährlich

Zugangsdaten, Schlüssel, Zertifikate und Tokens sind die unsichtbaren Verbindungsglieder moderner IT. Sie stecken in CI/CD-Pipelines, Konfigurationsdateien, Container-Images und Cloud-APIs. Und genau darin liegt das Risiko.

Klassische Sicherheitsarchitekturen haben jahrzehntelang auf Perimetersicherheit gesetzt: Wer im Netzwerk ist, gilt als vertrauenswürdig. Dieses Modell ist in Cloud-, Container- und Multi-Vendor-Umgebungen strukturell überholt.

Die Lösung heißt: “Zero Trust” – das Prinzip »Vertraue niemandem, überprüfe alles« – ist die architektonische Antwort darauf. Die Identität ist die schützenswerte Ressource: Nicht der Netzwerkstandort entscheidet über Zugriff, sondern die verifizierte Identität einer Person, Maschine oder eines Services – kombiniert mit dem Prinzip minimaler Rechte (Least Privilege).

Genau hier liegt der blinde Fleck vieler Unternehmen: Credentials, die nicht sicher verwaltet werden, untergraben jede Zero-Trust-Strategie von innen. Die kontinuierliche Überprüfung von Credentials wird zur Priorität.

Rund 38 % aller bestätigten Datenpannen begannen mit kompromittierten Zugangsdaten – Credential-basierte Angriffe brauchen im Schnitt 292 Tage, bis sie erkannt und eingedämmt werden.

Ein einziges gestohlenes Passwort reicht, um sich unbemerkt durch Ihr Netzwerk zu bewegen – Systeme zu manipulieren, Daten abzuziehen oder Produktionsprozesse zu stoppen.

Wie Credentials unkontrolliert wachsen

Das Problem entsteht nicht über Nacht – es wächst mit jedem neuen Projekt, jeder neuen Cloud-Instanz, jedem neuen Team. Typische Ausgangssituationen in Unternehmen:

- **Hardcodierte Passwörter:** Credentials direkt im Quellcode oder in Konfigurationsdateien – ein Git-Commit reicht, um sie öffentlich zu machen.

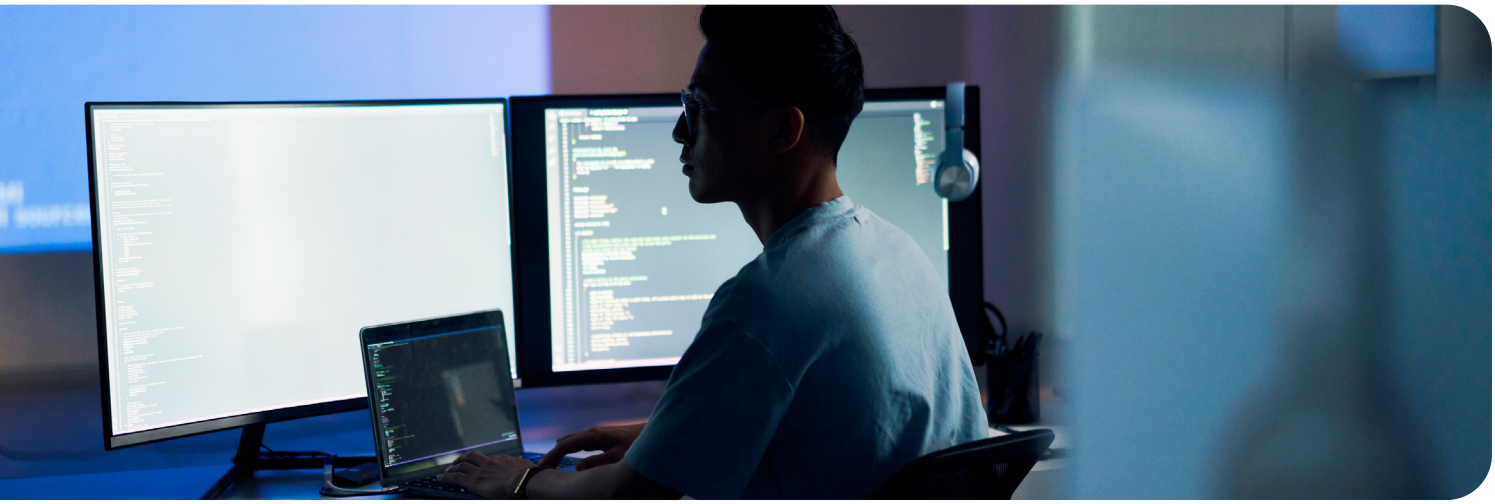
- **Geteilte Admin-Konten:** Ein Zugang, genutzt von 10 Personen – keine Nachvollziehbarkeit, keine individuelle Abrechenbarkeit.
- **Vergessene Zugänge:** Service-Accounts oder API-Keys, die nach Projektende oder Ausscheiden eines Mitarbeiters oder Projektpartners nie deaktiviert wurden.
- **Abgelaufene Zertifikate:** Zertifikate, die unbemerkt ablaufen und Produktionsausfälle verursachen.
- **Credentials per Chat / E-Mail:** Weitergabe über unsichere Kanäle – ohne Protokollierung, ohne Kontrolle.

Warum das ein C-Level-Thema ist

Die Folgen eines kompromittierten Credentials sind nicht nur technischer Natur. Sie treffen das gesamte Unternehmen:

- **Haftungsrisiko:** CISOs und das Management tragen die Verantwortung für Sicherheitslücken gegenüber Regulatoren und Aufsichtsbehörden.
- **Reputationsrisiko:** Ein öffentlicher Sicherheitsvorfall beschädigt das Vertrauen von Kunden, Partnern und Investoren – oft langfristig.
- **Compliance-Risiko:** NIS2, ISO 27001, BSI-Grundschutz und branchenspezifische Regularien verlangen nachweisbare Kontrolle über alle Zugriffe.
- **Geschäftsunterbrechung:** Produktionsausfälle durch abgelaufene Zertifikate oder gesperrte Zugänge kosten Geld – und Nerven.
- **Betriebsaufwand:** Manuelle Credential-Rotation, Audit-Vorbereitung und Incident Response binden IT-Ressourcen, die anderswo dringend gebraucht werden.

Die entscheidende Frage ist nicht: »Haben wir ein Problem?« sondern: »Wissen wir, was es uns wirklich kostet?«



Kapitel 2: Warum klassische Ansätze an ihre Grenzen stoßen

Viele Unternehmen verwalten Zugangsdaten mit Werkzeugen, die für eine andere Zeit gebaut wurden: Passwortmanager für einzelne Nutzer, Excel-Tabellen für Teams, manuelle Rotationsprozesse für Compliance-Audits. Diese Ansätze haben eines gemeinsam – sie skalieren nicht.

Das Fragmentierungsproblem

In gewachsenen IT-Landschaften entstehen Credentials-Silos: Entwicklung nutzt eigene Tools, Betrieb einen anderen Passwortmanager, Security wiederum eigene Prozesse. Das Ergebnis:

- **Keine zentrale Transparenz:** Niemand kann verlässlich sagen, wo welche Credentials existieren und wer Zugriff hat.
- **Keine einheitlichen Richtlinien:** Jedes Team definiert eigene Standards – oder hat gar keine.
- **Hoher manueller Aufwand:** Rotation, Genehmigungen und Audits verschlingen wertvolle Arbeitszeit.
- **Blinde Flecken im Audit:** Lückenhafte Protokollierung macht Compliance-Nachweise zum Kraftakt.

Statische Credentials: Ein Widerspruch zu Zero Trust

Moderne IT-Umgebungen sind hochdynamisch: Cloud-Instanzen entstehen und verschwinden in Minuten, Container werden bei jedem Deployment neu erzeugt, APIs kommunizieren automatisiert miteinander. In diesem Kontext sind statische, langlebige Zugangsdaten nicht nur ein operatives Risiko – sie widersprechen fundamental dem Zero-Trust-Prinzip.

Zero Trust fordert kontinuierliche Verifikation jeder Identität. Statische Credentials leisten genau das Gegenteil: Sie setzen blindes Vertrauen in ein Passwort, das einmal vergeben und selten hinterfragt wird.

- **Zu lange gültig:** Ein Credential, das Monate oder Jahre lang gültig ist, gibt Angreifern ein langes Zeitfenster.
- **Zu weit verbreitet:** Einmal geteilt, ist unklar, wer wirklich Zugriff hat und hatte.
- **Nicht rotiert:** Manueller Aufwand führt dazu, dass Rotation unterbleibt oder zu selten passiert.
- **Nicht auditierbar:** Wer hat wann mit welchem Credential auf was zugegriffen? – oft nicht zu beantworten.

Der versteckte Kostentreiber: Betriebsaufwände ohne Plattform

Was Secrets-Management ohne zentrale Plattform kostet, wird in Budgetplanungen selten sichtbar gemacht – obwohl die Aufwände real und erheblich sind. Sie verteilen sich auf viele Schultern: Entwickler, Administratoren, Security-Teams, Compliance-Beauftragte.

Manuelle Credential-Rotation
Jedes Passwort, jedes Zertifikat, jeder API-Key muss manuell identifiziert, geändert und in allen betroffenen Systemen aktualisiert werden.

Audit-Vorbereitung
Ohne zentrale Protokollierung müssen Logs aus verschiedenen Quellen mühsam zusammengeführt werden – in der Praxis oft 2–4 Wochen Vorbereitungszeit vor jedem externen Audit.

Incident Response
Wird ein Credential kompromittiert, beginnt eine aufwändige Analyse: Welche Systeme waren betroffen? Welche Credentials müssen gesperrt werden? Ohne Überblick dauert das Tage.

Onboarding & Offboarding
Neue Teammitglieder erhalten Zugänge manuell, ausscheidende Mitarbeiter werden nicht vollständig deaktiviert – ein dauerhaftes Sicherheits- und Compliance-Risiko.

Zertifikatsmanagement
Abgelaufene Zertifikate verursachen Produktionsausfälle – weil kein automatisches Monitoring existiert und Rotation manuell angestoßen werden muss.

Wissenssilos & Abhängigkeiten
Credential-Wissen konzentriert sich auf einzelne Personen – fällt die Person aus, entstehen kritische Engpässe im Betrieb.

Eine realistische Rechnung: Unternehmen mit 50–200 Systemen verbringen ohne Automatisierung schätzungsweise 20–40 Personentage pro Jahr allein für Credential-Rotation und Audit-Vorbereitung. Hinzu kommen ungeplante Aufwände durch Incidents und Zertifikatsausfälle – die in dieser Rechnung noch nicht enthalten sind.

Was wäre, wenn Sicherheit kein Engpass wäre, sondern ein Enabler?

Genau das ist der Anspruch von HashiCorp Vault! Sicherheit automatisieren, standardisieren und in den normalen Workflow integrieren – ohne Reibungsverluste für Entwickler und Operations. Die Investition in eine zentrale Plattform amortisiert sich nicht nur über abstrakte Sicherheitsgewinne, sondern auch über klar messbare Effizienzgewinne im laufenden Betrieb.

Kapitel 3: Der Vault-Ansatz: Zentral, dynamisch, automatisiert

HashiCorp Vault ist keine klassische Passwortverwaltung – es ist eine Secrets-Management-Plattform, die Sicherheit als automatisierten, reproduzierbaren Prozess versteht. Der Kern der Philosophie: Kein Credential sollte länger existieren als unbedingt nötig.

Technisch arbeitet Vault mit einem klar strukturierten Modell: Jede Entität – Mensch, Maschine oder Service – authentifiziert sich zunächst gegenüber HashiCorp Vault und erhält ein kurzlebiges Token. Dieses Token ist an Policies gebunden, die exakt definieren, auf welche Pfade und Aktionen Zugriff besteht. Alle Daten werden durch eine interne Verschlüsselungsschicht (die sogenannte "Barrier") gesichert, bevor sie im Storage Backend landen – selbst ein direkter Angriff auf den Storage-Layer liefert einem Angreifer nur verschlüsselte Daten.

Drei Grundprinzipien

Dynamische Credentials: Vault generiert kurzlebige Zugangsdaten on-demand – automatisch, für die Dauer eines Vorgangs, dann werden sie ungültig. Kompromittierte Credentials werden praktisch wertlos.

Zentrales Kontrollmodell: Eine Plattform, eine Policy-Sprache, ein Audit-Log – für alle Teams, Clouds und Workloads. Kein Silo, keine Ausnahme.

Identity-basierter Zugriff: Vault authentifiziert Maschinen, Services und Menschen über deren Identität. Jede Entität bekommt nur, was sie braucht (Least Privilege).

Vault als zentraler Baustein einer Zero-Trust-Architektur

Zero Trust ist kein Produkt, das man kauft – es ist ein Architekturprinzip, das konsequent umgesetzt werden muss. Vault adressiert dabei einen der drei zentralen Pfeiler: die Absicherung von Machine Identity und Secrets. Jede Entität – ob Anwendung, Pipeline oder Cloud-Workload – authentifiziert sich gegenüber Vault über ihre verifizierte Identität, erhält nur die minimal notwendigen Rechte, und nur für den definierten Zeitraum. Nach Ablauf dieses Zeitraums erlischt der Zugriff automatisch.

Zero Trust in der Praxis bedeutet: kein implizites Vertrauen, keine dauerhaften Credentials, kein Zugriff ohne Kontext. Vault setzt genau das technisch um – automatisiert, auditierbar und skalierbar. Damit wird Vault zum operativen Fundament jeder Zero-Trust-Strategie, die über Netzwerksegmentierung hinausgeht.

Das Herzstück von Vault sind sogenannte Secrets Engines – modulare Komponenten, die Secrets speichern, generieren oder verschlüsseln. Jede Engine ist auf einen spezifischen Anwendungsfall optimiert:

Database Secrets Engine: Generiert datenbankspezifische Zugangsdaten dynamisch auf Anfrage – mit konfigurierbarer Gültigkeitsdauer und automatischer Rotation. Services müssen keine Credentials mehr hardcodieren; jede Instanz erhält einzigartige Zugangsdaten, die nach Ablauf automatisch widerrufen werden.

PKI Secrets Engine: Stellt dynamische X.509-Zertifikate aus, ohne manuelle CSR-Prozesse oder CA-Wartezeiten. Zertifikate können im Arbeitsspeicher gehalten und beim Shutdown verworfen werden – kein Schreiben auf Disk, keine Zertifikats-Datenbank.

Cloud Secret Engines: Generiert kurzlebige Cloud-Credentials für AWS, Azure und GCP on-demand – basierend auf definierten IAM-Policies. Credentials werden automatisch widerrufen, wenn der Vault-Lease abläuft.

Transit Secrets Engine: Verschlüsselung als Service: Vault ver- und entschlüsselt Daten, ohne sie selbst zu speichern. Entwickler nutzen kryptografische Funktionen, ohne eine eigene Schlüsselverwaltung implementieren zu müssen.

KV Secrets Engine: Sicherer Key-Value-Store für statische Secrets mit optionaler Versionierung – bis zu 10 Versionen pro Key, mit Soft-Delete und Wiederherstellbarkeit.

Audit Logging: Jede Anfrage und Antwort wird lückenlos an den Audit Broker weitergeleitet – unveränderlich, exportierbar, SIEM-fähig.

Technologieagnostisch und zukunftssicher

Vault funktioniert On-Premises, in der Private Cloud und in Multi-Cloud-Umgebungen. Es lässt sich in bestehende Tools integrieren – GitLab, GitHub, Jenkins, Azure DevOps, Terraform, etc. – ohne dass bewährte Prozesse komplett neu gebaut werden müssen.

**Vault wächst mit Ihrer IT mit.
Von ersten Projekten in kleinen Teams bis zur globalen Enterprise-Infrastruktur – die Architektur skaliert, ohne dass Grundprinzipien geändert werden müssen.**

Sicherheit als Teil des Workflows – nicht neben ihm

Der entscheidende Unterschied zu klassischen Ansätzen: Vault integriert sich in DevOps-Prozesse, statt sie zu unterbrechen. Entwickler erhalten automatisch die richtigen Credentials zum richtigen Zeitpunkt – ohne Tickets, ohne Wartezeit, ohne manuelle Weitergabe. Sicherheit wird zum selbstverständlichen Teil jedes Deployments.

Kapitel 4: Drei Use Cases aus der Praxis

Abstrakte Sicherheitsversprechen helfen wenig – entscheidend ist, wie Vault in realen Unternehmensumgebungen wirkt. Hier sind beispielhaft drei typische Szenarien, die wir in unseren Projekten regelmäßig adressieren.

Praxisbeispiel GitHub: Kubernetes, CI/CD und dynamische Secrets in großem Maßstab

Ausgangslage:
GitHub betrieb ein gewachsenes, selbst entwickeltes Secrets-Management-System. Jede Änderung an statischen Credentials erforderte manuelle Anpassungen in allen verbundenen Systemen und Diensten – ein enormer Aufwand bei Dutzenden von Kubernetes-Clustern.

Lösung mit Vault:
Vault ersetzt das manuelle System vollständig: Secrets werden bei jedem App-Deployment automatisch injiziert, Zertifikate und Zugriffskontrollen über Vaults PKI-Engine verwaltet. Die Kubernetes-Cluster werden zentral über Vault gesteuert.

Ergebnis:
GitHub verarbeitet heute mehrere hunderttausend Secrets-Anfragen pro Tag automatisiert. Das Team, das zuvor die manuelle Lösung wartete, kann sich stattdessen strategischen Projekten widmen.

Praxisbeispiel ABN AMRO: Hard-codierte Credentials eliminieren – Banking und Container-Plattform

Ausgangslage:
Das 400-köpfige CISO-Team der niederländischen Großbank ABN AMRO stand vor einer typischen Enterprise-Herausforderung: hardcodierte Credentials in intern entwickelten Anwendungen und Skripten, ein on-premises Secrets-System mit hohem manuellem Aufwand, und der Druck, eine cloud-native Container-Plattform sicher aufzubauen.

Lösung mit Vault:
Nach einem Proof of Concept durch das CISO-Team führte ABN AMRO Vault als zentrales Secrets-Repository ein. Vault eliminiert manuelle Policy-Anwendungen auf neue Anwendungen und Hosts – und ermöglicht schnelles Onboarding auf die Container-Plattform dank des Vault Secrets Injector.

Ergebnis:
»Vaults dynamische Secrets und API-Verschlüsselung ermöglichen es, Anwendungen auf unserer Container-Plattform mit einem Bruchteil des bisherigen Zeit- und Arbeitsaufwands zu integrieren.« (Ton van Dijk, Agile Product Owner Identity & Access, ABN AMRO)

Praxisbeispiel athenahealth: Betriebseffizienz und Hochverfügbarkeit im Gesundheitswesen

Ausgangslage: athenahealth, ein US-amerikanischer Anbieter von Healthcare-IT, schützt mit seinen Systemen Hunderte Millionen Patienten- und Geschäftsdaten. Das bestehende Secrets-Ticketsystem war aufwändig, fehleranfällig und verursachte bei Verfügbarkeitsproblemen Lösungszeiten von bis zu vier Stunden.

Lösung mit Vault: athenahealth konsolidierte Tausende von Secrets in Vault und verteilte sie von dort standardisiert an Web-, Datenbank- und Anwendungsserver. Vault ermöglicht einheitliche Secrets-Policies und Self-Service-Optionen für einzelne Teams – ohne Ticketsystem.

Ergebnis: Das Secrets-Ticketsystem wurde praktisch eliminiert. Verfügbarkeitsprobleme werden seither in unter 30 Minuten statt in vier Stunden behoben. »Vault hat sich als großer Gleichmacher erwiesen – es hilft, die Balance zwischen Datensicherheit und minimalem Aufwand zu finden.« (Ganapathysaran Nambirajan, Senior Engineering Manager, athenahealth)

Kapitel 5: Der Weg zur Zielarchitektur – Ihr Reifegradmodell

Kein Unternehmen transformiert seine Sicherheitsarchitektur über Nacht. Erfahrungsgemäß verläuft der Weg von fragmentierten Einzellösungen zur integrierten Identity-Plattform in drei klar abgrenzbaren Phasen – mit jeweils eigenem Fokus und messbarem Fortschritt.

Phase 1: Transparenz schaffen

→ Bestandsaufnahme
→ Analyse bestehender Zugriffspfade
→ Identifikation kritischer Risikobereiche
→ Vault-Pilotprojekt im ersten Scope

Phase 2: Zentralisieren & automatisieren

→ Einführung dynamischer Credentials
→ Ablösung statischer Passwörter
→ Policy-Framework etablieren
→ CI/CD-Integration umsetzen

Phase 3: Skalieren & integrieren

→ Multi-Cloud-Rollout
→ Kubernetes-Anbindung
→ SIEM/Audit-Integration
→ Unternehmensweite Governance

Der Dreiphasen-Ansatz ermöglicht es, schnell sichtbare Ergebnisse zu liefern – ohne monatelange Vorprojekte. Phase 1 schafft in wenigen Wochen Klarheit über das tatsächliche Risiko. Phase 2 bringt die erste operative Sicherheitsverbesserung. Phase 3 transformiert die gesamte Sicherheitsarchitektur.

Wir begleiten Sie durch alle drei Phasen. Von der initialen Risikoanalyse über die Vault-Implementierung bis zum Betrieb – als HashiCorp-Partner kennen wir die Stolpersteine und wissen, wie man sie vermeidet.

Was wir in unseren Projekten gelernt haben

- **Transparenz ist der Schlüssel:** Unternehmen unterschätzen systematisch, wie viele Credentials existieren und wo sie stecken.
- **Schnelle Wins motivieren:** Ein erfolgreiches Pilotprojekt in einem kritischen System schafft interne Akzeptanz für die weitere Transformation.
- **Governance von Anfang an:** Teams, die Policies frühzeitig definieren, vermeiden spätere Nacharbeiten und Ausnahme-Regelungen.
- **Betrieb mitdenken:** Vault muss nicht nur implementiert, sondern auch betrieben werden – Hochverfügbarkeit, Monitoring und Backup-Prozesse sind Teil der Lösung.

Fazit: Sicherheit ist kein Projekt – sie ist eine Plattform.

Zero Trust ist kein Marketingbegriff – es ist ein Framework, das den Aufbau der Architektur bestimmt! Secrets- und Identity-Management ist dabei das operative Fundament: Ohne sichere, verifizierte und kurzlebige Identitäten für Maschinen und Services bleibt Zero Trust ein strategisches Versprechen ohne technische Substanz. HashiCorp Vault liefert genau diese Substanz – skalierbar, auditierbar und integrierbar in jede bestehende IT-Landschaft.

Was Sie mitnehmen sollten:

- ✓ Statische Credentials sind ein strukturelles Risiko– dynamische, kurzlebige Zugangsdaten sind der neue Standard.
- ✓ Manuelles Secrets-Management ist ein versteckter Kostentreiber– 20–40 Personentage pro Jahr allein für Rotation und Audits sind keine Seltenheit.
- ✓ Fragmentierung kostet Zeit und Sicherheit– eine zentrale Plattform schafft Transparenz und reduziert Komplexität.
- ✓ Compliance wird reproduzierbar– automatisierte Protokollierung und Policies machen Audits planbar statt reaktiv.
- ✓ Vault skaliert von Pilot bis Enterprise – ohne Technologiebruch.
- ✓ Vault ist ein zentraler Baustein von Zero Trust– Identity-basierter Zugriff, Least Privilege und kurzlebige Credentials machen Zero Trust operativ umsetzbar.
- ✓ Der Weg beginnt mit Transparenz – eine strukturierte Bestandsaufnahme zeigt, wo der größte Handlungsbedarf besteht.

Ihr nächster Schritt: Vault Security Workshop

In einem halbtägigen Workshop analysieren wir gemeinsam Ihre aktuelle Secrets-Landschaft, identifizieren die größten Risikobereiche und zeigen Ihnen einen konkreten Fahrplan zur Vault-Einführung – zugeschnitten auf Ihre IT-Umgebung.

Termin buchen

DIE PROFI ENGINEERING SYSTEMS AG

Die PROFI AG ist ein mittelständischer IT-Dienstleister mit Unternehmenssitz in Darmstadt. Das Unternehmen begleitet seine Kunden in allen Belangen der digitalen Transformation mit einem spezialisierten Portfolio von IT-Lösungen, Dienstleistungs- und Beratungsangeboten rund um die Themen Server- und Speichersysteme, Hybrid Cloud, Business Continuity, Cyber Resilience, IT-Automation, Virtualisierung, Digital Workplace, Software-Entwicklung und Managed Services.

Der Anspruch ist höchste Kompetenz, Zuverlässigkeit und Qualität, mit messbarem Erfolg und direktem Beitrag zur Wertschöpfung und Wettbewerbsfähigkeit der Kunden.

PROFI beschäftigt über 300 Mitarbeitende an bundesweit 12 Standorten. Seit vielen Jahren gehört das Unternehmen zu Deutschlands erfolgreichsten IT-Lösungsanbietern und pflegt langjährige Partnerschaften mit allen führenden IT-Herstellern.

Unsere IT-Lösungen für Ihren Erfolg

- **Business Continuity**
- **Cyber Resilience**
- **DevOps**
- **Digital Workplace**
- **KI**
- **Managed Services**
- **Netzwerk / IT Security**
- **Platforms**
- **SDDC / IT-Automation**
- **Software-Entwicklung**

05/2026

PROFI Engineering Systems AG
Otto-Röhm-Straße 18
64293 Darmstadt
Telefon: +49 6151 8290-0
Telefax: +49 6151 8290-7610
E-Mail: profi@profi-ag.de
www.profi-ag.de

UNSERE PARTNER

Gemeinsam mit unseren starken Partnern setzen wir Ihre optimalen Lösungen um.

PROFI
Wir entwickeln mehr als IT