5.12.2018

F-IT 4 PAM

Effizienter IT-Betrieb trotz und mit Privileged Access Management

Christoph Franke
F-IT Security and Audit GmbH

Unser Angebot

Unter unserer Marke **Audit4u** bieten wir eine ganzheitliche Dienstleistung rund um die Thematik Privileged Access Management (PAM) an und der – oftmals übersehene bzw. ausgeblendete – Aspekt im IT-Betrieb des „nicht privilegierten Zugangs“.

Unser Grundgedanke orientiert sich an der Sicherung des geordneten und effizienten IT-Betriebs unter Berücksichtigung der regulatorischen Anforderungen. Reflexhafte Maßnahmenerledigung, ohne die betrieblichen Notwendigkeiten oder Einschränkungen gebührend zu berücksichtigen, werden sie von uns nicht erhalten.

Die Qualität unserer Leistung ist an den Anforderungen des BAFin sowie der EZB zu messen, wobei selbstverständlich auch die Anforderungen von BAIT, GDPR/DSGVO und BetrVG berücksichtigt werden. Zusatzanforderungen weiterer Regulatoren des Finanzmarktes wie beispielsweise CSSF, MAS oder FED bzw. der Regulatoren anderer Branchen sind uns wohl bekannt und können bei Bedarf in der Lösungsfindung integriert werden.

Der Lösungsentwurf ist nicht auf den Finanzsektor beschränkt ist, da die Problemstellung auf viele Branchen mit sensiblen Daten in der IT-Infrastruktur leicht transformiert werden kann.

Inhalt:

Vorgehensweise

Das folgende Phasenmodell vermittelt einen ersten Einblick, wie wir die Komplexität des Vorhabens zur Implementierung eines regulatorisch wie betrieblich angemessenen „Privileged Access Management“, in Teilaufgaben zerlegen. Schrittweise und somit beherrschbar erfolgt die Risikoreduzierung und die kontinuierliche Eingliederung in ein ISMS[1] steigert den Reifegrad der Organisation.

Phasenmodell

1. Definition der Anforderungen an eine PAM-Lösung (gestützt auf ggf. vorhandenen Moniten und ausgerichtet an "good practices[2]") zur Einpassung in das bestehende oder in Aufbau befindliche ISMS
2. Grobentwurf eines Lösungsmodells unter Berücksichtigung der von Ihnen vorgegebenen Rahmenbedingungen (ITIL-Konformität, ISMS, Arbeitnehmervertretung, Datenschutzregelungen)
3. Aufnahme der existierenden Kontrollen, IT-Management- und IT-Administrations-Prozesse sowie der vorhandenen Umsysteme mit Zulieferungen für das Umsetzungsmodell
4. Projektplanung inkl. des IAM[3]-Modells, des Architektur-Designs und der Umsetzungs- wie Rollout-Planung
5. Definition von IAM-Anforderungen (taktisch vs. strategisches Vorgehen zur Einbindung in die existierende IAM-Landschaft; Abwägung der geforderten / gewünschten Anpassungen; dies umfasst JML[4]-Prozesse, Ownership-Klärung – Rollen vs. Personalized Access, Revalidierung)
6. Entwurf des Kontrollumfelds (Befugnisse, Regeln, Ausnahmen, Eskalationen, Protokollierung, SIEM, Session-Recording, Nachschau, Notfall Zugriff…)
7. Unterstützung beim Proof-of-Concept der technischen Komponenten für die PAM-Lösung in allen Phasen bis zur Entscheidungsvorlage
8. Architektur-Feindesign, Implementierungsplanung der PAM-Lösung, Prozessplanung für den Betrieb
9. Implementierung der PAM-Lösung inkl. Pilotierung zum Nachweis der technischen Machbarkeit
10. Einführung der unterstützenden Prozesse für den Betrieb der PAM-Lösung
11. Koordinierter Rollout – gestaffelt nach Priorität für OS- oder DB-Level oder Application-Level – Use-Cases, Rollenmodellierung, Zugangsarchitektur, Regeln, Implementierung, Early-Live-Support
12. Abgrenzen und heben von Synergien mit möglichen parallel laufenden Projekten, wie Database Activity Monitoring
13. Überführung der PAM-Lösung in den Produktivbetrieb
14. Review des Betriebs (Application Management und -Operations der PAM-Lösung, IAM-JML-Integration, technologische Fortschreibung, Integration in IT-Releasemanagement, Disaster Recovery, BCM, …) zur Bewertung der Nachhaltigkeit
15. Pilotierung einer Analyse der vielfältig erzeugten Daten, die im Rahmen der PAM Initiative erzeugt wurden, um zielgerichtet mögliche Vergehen zu identifizieren

[1] Information Security Management System
[2] Best practice ist das Ambitionsniveau , jedoch sollte good practice als hinreichend betrachtet werden
[3] IAM – Identity & Access Management
[4] JML – Joiner Mover Leaver-Prozess

Alleinstellungsmerkmale unseres Vorgehens

production first
Der Fokus ist nicht, Administratoren zu behindern, sondern den geordneten und sicheren IT-Betrieb technisch so abzusichern, dass ein Niveau hinsichtlich des operationellen Risikos erreicht wird, das den regulatorischen Anforderungen genügt. Dies ist keine Einschränkung der PAM-Kontrollen, sondern erfordert tiefes Verständnis in die Anforderungen des Tagesbetriebs (inkl. Change Implementierung) wie auch bei der Behebung von Vorfällen (Incidents) bis hin zu Großschäden (Desaster Recovery), um den effizienten Arbeitsbereich der IT-Betriebseinheiten innerhalb des angestrebten Risikoniveaus zu finden.

adopted control level
Wir stimmen mit ihrem Haus die Mischung aus verhindernden, aufdeckenden, wie bedarfsgetriebenen Kontrollen (preventative, detective, forensic controls) ab.

Die Balance zwischen Einmalinvestitionen und den fortlaufenden Kosten im Realbetrieb ist eines der wichtigsten Kriterien beim Entwurf der Lösung innerhalb der vorgegebenen Grenzen des angestrebten Sicherheits- bzw. Risikoniveaus.

accept your environment
Die ungeliebten und oft unterbewerteten Problembereiche wie Datenqualität in ITSM-Systemen, Prozessdisziplin in der Administration, Pseudo-SIEM-Coverage werden beim Design der PAM-Lösung ebenso berücksichtigt wie Schwachstellen in den IAM-Prozessen.

no secondary agenda
Wir arbeiten ohne Produktpräferenzen, sind jedoch mit diversen Herstellern eng verbunden und können auf deren „technical Presales“ zurückgreifen.

Provisionsfreiheit wird – gerne auch formal/vertraglich – zugesichert.

widely spread skillset
Das Team besteht nicht nur aus IT-Security-Experten, sondern bringt sowohl technologische Kenntnisse wie Erfahrung aus dem IT-Produktionsbetrieb („Operations/Delivery“) mit und verfügt über Erfahrungen aus der Arbeit im IT-Produkt-Management (Release-, Feature-Management, Customizing, Migration) neben den IT-Security- und IT-Audit bezogenen Erfahrungen sowie den profunden Kenntnissen in der Steuerung und Abwicklung von komplexen Integrationsprojekten.

early handover to you
Die frühe Überführung in den Betrieb (auch für Rollouts), senkt die externen Kosten bei Inanspruchnahme und führt zur frühzeitigen Stabilisierung des Betriebs.

Dies bedeutet nicht, dass wir sie mit einem Piloten „allein lassen“, sondern dass es ihre Entscheidung ist, unsere Unterstützung sachgerecht zu reduzieren oder zu beenden.

"Nachteile" unseres Vorgehens:

plan hits reality

Die Planung der PAM-Lösung in die bestehende IT-Ablauf-Organisation unter Nachweis der existierenden Gaps führt ggf. zu Parallelprojekten, die notwendigen Grundlagen schaffen müssen. Zur Entzerrung und Verteilung der Investition sind gestufte Pläne für das PAM-Projekt gegebenenfalls angeraten.

fit for purpose

Die Adaption der PAM-Lösung an bestehende Erfordernisse die Produktion zu sichern, führt in der Planungs- und Implementierungsphase ggf. zu verlängerten Detailplanungs- bzw. Customizing-Phasen.

we are not on a green field

Die Komplexität, das bestehende Risiko zu bearbeiten wie auch notwendige flankierende Maßnahmen, eine wirklich wirksame Lösung zu implementieren, wird früh transparent gemacht. Kompromisspläne auf dieser Basis sind vereinbar.
Der Punkt ist, dass wir für Transparenz stehen, wenn Rahmenbedingungen zu Einschränkungen hinsichtlich der Wirksamkeit der PAM-Lösung führen werden.

love it, change it, or leave it

Der Nachteil für uns am Vorgehen liegt aufgrund unseres Anspruchs darin, dass wir bei organisatorischen Hemmnissen innerhalb ihrer Organisation, die die Mindestwirksamkeit der PAM-Lösung voraussichtlich verhindern würden, dies dokumentieren werden und von den Folgephasen Abstand nehmen werden.

Bitte bewerten sie selbst, ob dies wirklich "Nachteile" sind.

Wir freuen uns auf eine intensive Diskussion des Themas mit ihnen.

Details unseres Angebots

Verfügbare Skillsets

- ✓ **IT Security Architect**
- ✓ **IT Security Manager**
  Zertifizierung: CISM, CISSP,
- ✓ **I&A Specialist**
- ✓ **IT Security Governance Manager (Retained Organization)**
- ✓ **IT Software Architect**
- ✓ **IT Infrastructure Architect**
- ✓ **IT Auditor**
  Zertifizierung: CISA
- ✓ **SIEM specialist**
- ✓ **IT Risk Management Analyst**
- ✓ **IT Application Operations and Management Specialist**
  Zertifizierung: ITIL Foundation
- ✓ **IT infrastructure operations skills**
  Zertifizierung: ITIL Foundation
- ✓ **Software Product Manager**
- ✓ **Regulatory- and IT Audit Response Manager**
  Zertifizierung: CISA
- ✓ **Application Integration Specialist**
- ✓ **Process Analyst and Designer**
- ✓ **Senior Project Manager**
  Zertifizierung: PMI
- ✓ **PMO Specialst**

Erfolgsfaktoren, die sie beeinflussen können und sollten

Umfassende Informationen

Vorliegende Moniten beispielsweise der internen Revision, der beauftragten Wirtschaftsprüfer und der regulatorischen Institutionen (BAFin, EZB, …) werden zur Projektinitialisierungszeit der externen Projektleitung im Original zur Kenntnis gegeben und sind wichtige Planungsgrundlagen für das Vorhaben.

Während der aktiven Teilnahme am Vorhaben bieten wir an, Anfragen der entsprechenden Autoren (Revision, WP, …) – in Absprache mit ihnen – zu beantworten. Diese Zuarbeit ist nicht explizit zu kontrahieren, sondern Teil des Gesamtangebots,

Projekt vs. Linie

Ihre Verantwortung ist, dass die Zuarbeit aus der Linienorganisation, nach Abstimmung mit ihrer internen Projektleitung, gesichert ist.

Dies sollte nicht „top-down" erfolgen, sondern wir werden mit den betroffenen Abteilungen inkl. der Mitarbeiter in eine offene Kommunikation eintreten, um die Anforderungen aus dem realen IT-Betrieb im Vorgehensmodell als wesentlicher Faktor zu berücksichtigen.

Es sollte keine Isolierung zwischen dem Vorhaben und der laufenden IT-Betriebsorganisation stattfinden. Wir werden die Organisation von querschnittlichen Abstimmungsrunden zur Qualitätsverbesserung der Lieferungen des Vorhabens begrüßen und aktiv fördern.

Sie legen die Prioritäten fest und entscheiden auf Basis der von uns vorgelegten Optionen, welchen Weg das Projekt einschlagen soll, um Ihre Strategie umzusetzen.

Anmerkung:

Jegliche potenzielle Änderung auf die Projektdefinition wird von uns aufgenommen und nur nach formaler Bearbeitung eines PCR[5] von uns übernommen.

Professionelles Risk- und Issue-Management von nicht verabschiedeten PCRs wird von uns zugesichert.

Unsere Verantwortung und unser Anspruch

Wir berichten real und ohne politische Dimension im Rahmen des Projekt-Status-Reporting. Green-Shift ist keine Option für uns.

Wir scheuen uns nicht davor PCRs vorzuschlagen, wenn sie aus Erkenntnissen des realen IT-Betriebs, der Datenqualität von zuliefernden Systemen oder des Compliance-Level betroffener Prozesse ausgelöst werden.

Wir verzichten auf teure Marketing- und Vertriebswege, daher sind erfolgreiche Projekte und zufriedene Kunden unsere Erfolgsgaranten.

Anmerkung:

Umgekehrt lassen wir uns nicht daran messen, ob PCRs genehmigt werden, denn die Behebung der Ursache eines PCR außerhalb des Projekts kann eine bessere Lösung sein und hilft dem Vorhaben dennoch.

Wir sichern zu, den Auslöser jedes PCR anhand von nachvollziehbaren Fakten zu belegen.

[5] Project Change Request

Details zur Implementierung

PAM Enforcement

Die Restriktion der Nutzung privilegierter Rechte kann nur sichergestellt werden, wenn das sogenannte „Enforcement“ in allen Betriebszuständen wirksam ist.

Aufgrund der vorliegenden Infrastruktur, der Netzwerksegmentierung oder anderen Gegebenheiten sind Situationen denkbar, die die Wirksamkeit einschränken. In diesen Fällen werden im Rahmen des Lösungsdesigns, entweder die Rahmenbedingungen verändert oder für solche Use-Cases die verhindernde Kontrolle (preventative control) in eine aufdeckende Kontrolle (detective control) modifiziert, um prozessual oder organisatorisch eine Kompensation zu erreichen.

Anmerkung:
Diese Abwägung – gestützt auf Informationen aus den IT-Betriebseinheiten – ist wesentlich, denn sie bestimmt gegebenenfalls die (negativen) betrieblichen Aspekte von PAM (verlängerte Reaktionszeiten, erhöhter Personalaufwand, Personalfrustration).

Implementierungsmuster

Preventative Access Restriction
Der Netzwerkzugang zu IT-Assets unterliegt einer Kontrolle auf Netzwerkebene (Layer 3 bis 7), um sicherzustellen, dass nur gerechtfertigte Zugangsanfragen zugelassen werden.
Die Implementierung erfolgt über Firewalls oder Proxys.
Notwendig ist hierzu eine wirksame Netzwerksegmentierung (Client- vs. Server-Segmente).

Detective Access Detection
Sofern die Nutzung der PAM-Infrastruktur technologisch umgehbar ist, werden nachgelagerte Kontrollen – beispielsweise durch SIEM-Systeme – implementiert, um solche Vorgänge der Klärung zuzuführen.

Preventative Credential Restriction
Die Bereitstellung der secret authentication information (credentials) wird an die Rechtfertigung des Zugangswunsches gebunden.
Die Implementierung erfolgt in der Regel über Verwaltung der credentials in einem Enterprise Password Vault (EPV), der mit der PAM-Lösung gekoppelt ist.

Detective Credential Usage
Sofern die credentials auch ohne Nutzung der PAM-Lösung verfügbar sind, beispielsweise durch manuellen Check-Out von Kennwörtern aus dem EPV oder durch Nutzung unerlaubt gespeicherter SSH-Schlüssel, sollte dies über nachgelagerte Kontrollen – beispielsweise SIEM – aufgedeckt und der Klärung zugeführt werden.

Centralized Enforcement
Der technische Zugang erfordert es, dass eine Kontrolle der PAM-Lösung dies gestattet.

Referencing Enforcement
Bei jedem Zugangsbegehren wird das IT-Asset sich rückversichern, dass eine Genehmigung bei der zentralen PAM-Lösung vorliegt.

Local Enforcement
Es ist auf dem IT-Asset sichergestellt, dass das IT-Asset, zu dem Zugang begehrt wird, nur auf Basis einer genehmigten Anforderung den Zugang gestattet.

Technische Komponenten einer PAM-Infrastruktu

Kernkomponenten

Sichere Identifikation
Mitarbeiter, die privilegiert arbeiten, sollten durch Mehr-Faktor-Authentisierung identifiziert werden. Unter Effizienzaspekten sollten hierzu Single-Sign-On Mechanismen genutzt werden.

***Entscheidungslogik*,**
Dies ist die zentrale Stelle, an der das definierte *PAM-Regelwerk* technisch durchgesetzt wird.

***Eskalationsmechanismus*,**
Für den Fall, dass das Regelwerk nicht uneingeschränkt anwendbar ist, empfehlen dringend einen leichtgängigen und permanent verfügbaren Ablauf technologisch zu implementieren, der die Übersteuerung der PAM-Kontrollen durch eine vom Administrator unabhängige weitere Person zu gestatten.

Credential Store
Um die Nutzung privilegierter Accounts dem PAM-Regelwerk zu unterwerfen, werden deren Kennwörter, SSH-Private-Keys und Client-Auth-Zertifikate technisch kontrolliert. In der Regel wird die Anbindung einer Enterprise Password Vault Technologie sich aufdrängen.

***Enforcement Points*,**
Um die Umgehung der PAM-Lösung verhindern, werden Enforcement Points implementiert. Die Gestaltung ist mindestens abhängig von den Technologien der IT-Assets und der Netzwerk-Topologie. Wichtig ist hierbei neben der Wirksamkeit der Aspekt der Notfallvorsorge.

Protokollierungstechnologie
Die Nachvollziehbarkeit privilegierter Tätigkeiten sowohl bezüglich der PAM-Lösung als auch für die Tätigkeiten auf den IT-Assets ist ein wichtiges Kriterium zur Beurteilung des Risiko- bzw. Sicherheitsniveaus. Dies kann durch eine Session-Recording-Lösung unterstützt werden, jedoch ist dies nur eine Option.

Auskunftsfunktion
innerhalb der PAM-Lösung, um typische Fragestellungen zu klären. Beispielsweise „Wer hat am/um auf dem Server gearbeitet“, „Wer hatte den root-User zuletzt“, „Wer arbeitet manuell statt mit Bladelogic“, „Wann war der letzte privilegierte Vorgang auf dem Domain-Controller“ und auch „Wo war der Meier in der letzten Woche tätig“ [BetrVG!]

Notfallvorsorge
Da die PAM-Lösung ein IT-System ist, kann nicht von 100% Verfügbarkeit ausgegangen werden. Daher sind organisatorische wie technische Maßnahmen vorzuhalten, um bei einem Ausfall der PAM-Lösung den IT-Betrieb aufrecht zu erhalten. Gestufte Modelle sind angeraten.

Zuliefernde Umsysteme

IAM-Systeme

Innerhalb der IAM-Systeme sollte abfragbar sein, welche Accounts für IT-Assets einsetzbar sind und ggf. auf welchem Privilegienniveau (technische Rolle) sie autorisiert sind.
Implementierungsseitig ist ggf. auch die Ablage in Authentisierungssystemen wie AD, LDAP, RACF denkbar.

HR/Rollenmanagement

Anhand von HR-Daten, sollte die Zuordnung von Mitarbeiten zu Business-Roles verfügbar sein. Dies kann ersetzend auch in IAM-Systemen abgelegt sein.

CMDB

Wesentliche Informationen über die technischen IT-Assets werden benötigt, um die Entscheidungslogik zu versorgen. Dies sind neben Name, Lifecycle-Status, SDLC-Status, FQDN und Betriebssystem-Typ klarstellende Informationen wie zuständige Support-Teams, Wartungskalender sowie die Zuordnung zu IT-Service Assets bzw. Anwendungen.

Auftragsdatenbank

Anlehnend an das ITIL-Modell, sollten ungeplante privilegierte Aktivitäten wenigstens einer dokumentierten Ursache zuzuordnen sein (Incident), geplante hingegen einer freigegebenen Ursache (Change-, Service-Request). Die Referenzierung hinsichtlich IT-Asset stärkt die PAM-Kontrollen jedoch nur, wenn auch die CMDB die notwendigen Referenzdaten bereitstellt.

Zu versorgende Umsysteme

Archivierung

Aufbewahrungspflichtige Inhalte in Bezug auf die Nutzung privilegierter Rechte, sind anforderungsgemäß zu archivieren und zu löschen.
Konzeptionell ist dafür zu sorgen, dass dies sowohl Vorgangs-, IT-Asset- wie Mitarbeiterzentriert erfolgt.

Revalidierungssysteme

Es erscheint denkbar, die Rollen-Nutzung an Revalidierungssysteme weiterzugeben, um dem Entscheider für Account- oder Rollen-Revalidierung eine verbesserte Datenlage bereitzustellen. (Wird die Rolle wirklich genutzt?)

SIEM-Systeme

Die PAM-Lösung sollte die Metadaten zu autorisierten privilegierten Zugängen (IT-Asset, genutzter Account, Zeit, Auftrag) an eine SIEM-Lösung weitergeben, um dort die Korrelation mit Informationen vom IT-Asset zu gestatten. Dies verhindert false positives und fördert die Erkennungsquote für unerwünschte Aktivitäten.

Auftragsdatenbank

Optional sollte bedacht werden, ob die Auftragsdatenbank mit Metadaten zu autorisierten privilegierten Zugängen (IT-Asset, genutzter Account, Zeit) versorgt wird, um die Dokumentationslage – ohne manuelle Eingriffe – zu verbessern.

Abdeckung der IT-Technologie

Anders als viele Anbieter ist unser Modell nicht auf Windows, Unix und Linux limitiert.

Erfolgreich durch unser Team unter PAM-Kontrolle gestellte Technologien umfassen derzeit:

Betriebssystem-Typen:

- AIX
- i5/OS (AS/400)
- Linux x86
- Linux on Z
- Netzwerkkomponenten (mit RADIUS- oder LDAP-Authentisierung)
- NonStop Kernel (Tandem)
- Solaris
- Storage Devices (mit RADIUS- oder LDAP-Authentisierung)
- Windows Server
- z/OS mit RACF
- z/OS mit TopSecret

Datenbanksysteme

- MS SQL
- MariaDB / MySQL
- Oracle
- DB2 (i5, Windows, Linux, z/OS)

Anmerkung:
Lokaler Zugang via OS.

Hypervisors

- z/VM
- ESXi
- Anmerkung:
  Lokaler Zugang via OS.

Middleware-Komponenten

- Websphere MQ
- Websphere AS
- CICS TS

Client based IT-Infra-Admin Access

- rdp-client (mstsc) – *Jumphost nicht empfohlen*
- ssh client (putty) – *Jumphost nicht empfohlen*
- 3270 client (Quick3270, pcomm, opentext) – *Jumphost nicht empfohlen*
- CICS-Explorer –*Jumphost ggf. SSO*
- MQ-Explorer –*Jumphost ggf. SSO*
- Webbrowser – *Jumphost*

Anmerkung:
Grundsätzlich sind alle FAT-Clients anzubinden.
Hinsichtlich SSO ist zu untersuchen, welche Ausführungsplattform benötigt wird (für Windows haben wir eine Musterlösung).
Weiterhin ist die Untersuchung nötig, ob ein sogenannter „scripted Login“ oder eine Parameterübergabe möglich ist.

Enforcement bietet sich in allen Jumphost-Szenarien über dynamische Firewall-Regeln (z.B. Checkpoint, Juniper) oder ggf. als local / referencing enforcement an.

Client based IT-Appl-Admin Access

- MQ-Explorer –*Jumphost ggf. SSO*
- TOAD –*Jumphost ggf. SSO*
- Webbrowser – *Jumphost*

Anmerkung:
siehe „Client based IT-Infra-Admin Access“

Kontakt

Wir freuen uns auf eine intensive Diskussion mit Ihnen:

F-IT Security and Audit GmbH
Leinemühle 6
06343 Mansfeld

Ihr Ansprechpartner:

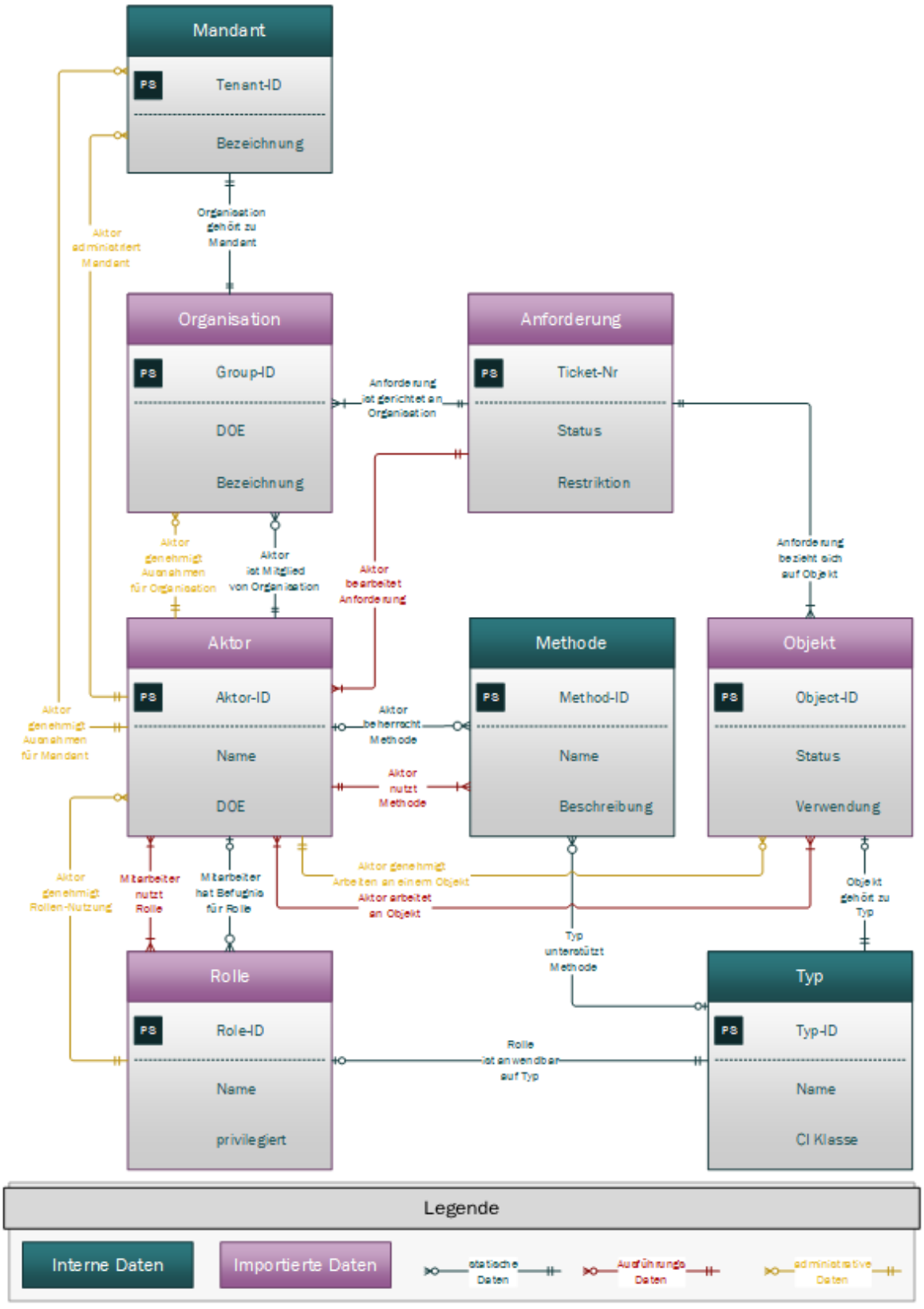
Dipl.-Inform. Christoph Franke
kontakt@f-it.biz

Web-Informationen:

http://www.f-it.biz
http://christoph.f-it.biz

Anhang – dies hilft zum weiteren „Eindenken“

Basismodell für privilegierten Zugang:



Grafische Darstellung des Gesamtvorgehens bei höchster Komplexität