PXM – Schutz und Verwaltung privilegierter Zugriffe

Unser Schutz für Ihre Operational Technology (OT) und Information Technology (IT).

www.tuv.com/informationssicherheit

TÜVRheinland®
Genau. Richtig.

Schutz privilegierter Zugriffe

UNTERSCHÄTZTE BEDROHUNG

Die Zugangsdaten von privilegierten Nutzern oder OT-Elementen sind eines der Hauptziele von Angreifern. Oftmals werden OT-Elemente nicht gegen Zugriffe geschützt oder es werden unveränderte Standardpasswörter benutzt. Sofern Administratorenkonten eingerichtet wurden, verwenden diese allzu oft gemeinsame Anmeldedaten mit offensichtlichen Benutzernamen und einfachen Passwörtern. Die professionelle Überwachung und Verwaltung von privilegierten Zugriffen und Zugriffs-/Benutzerdaten ist daher essentiell. Dieser Überwachung kommt durch die voranschreitende Verknüpfung von OT- mit IT-Netzwerken eine unternehmenskritische Bedeutung zu, da OT-Steuerungen durch die Verknüpfung der Netzwerke weltweit sichtbar und ansprechbar sind.

DIE LÖSUNG: PXM

Erst eine leistungsfähige Kombination (PXM) aus den unterschiedlichen Disziplinen PIM (Privileged Identity Management), PAM (Privileged Access Management) und PSM (Privileged Session Management) garantiert eine sichere Verwaltung von privilegierten Zugriffen und Benutzerkonten. Dieser kombinierte Einsatz setzt neue Maßstäbe für die Verwaltung von Zugriffen und die Verhinderung von Datenangriffen, sowohl in Ihrer Office-IT als auch im industriellen OT-Umfeld. Im Rahmen der kombinierten Disziplinen PIM und PAM wird die Gewährung privilegierter Zugriffsrechte mit rollenbasierter Zugriffsverwaltung und automatisierten Workflows sicher gesteuert. Weiterhin wird gewährleistet, dass Passworte nur zur Laufzeit vergeben werden und auch nur zur Laufzeit genutzt werden können.

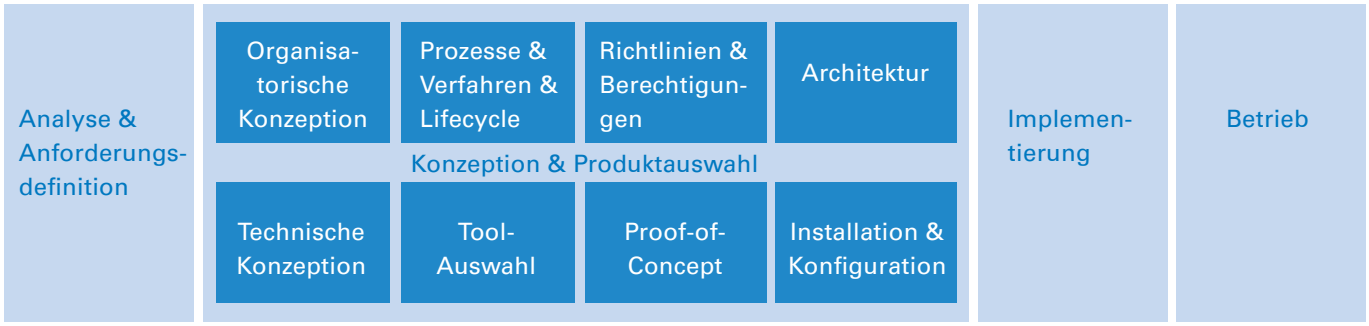

ABBILDUNG: UNSERE SERVICES UND UNSERE VORGEHENSMETHODIK

SCHRITT 1: ANALYSE UND ANFORDERUNGSDEFINITION

Analyse und Aufnahme der Anforderungen. Dies ist die Grundlage für die weiteren Schritte, um gemeinsam mit Ihnen die notwendigen Konzeptionen erstellen zu können.

SCHRITT 2: KONZEPTION UND PRODUKTAUSWAHL

Gemeinsam mit Ihnen planen unsere Experten welche Lösungskombination aus PIM, PAM und PSM notwendig ist. Neben der Lösungsarchitektur werden die notwendigen Technologien, Prozesse, Richtlinien und Lifecycle spezifiziert. Ziel ist die ganzheitliche Kontrolle der privilegierten Zugriffe.

SCHRITT 3: IMPLEMENTIERUNG

Unsere Experten installieren gemeinsam mit Ihnen die ausgewählten Lösungen in Ihrer Umgebung und sorgen für eine problemlose Übergabe in den produktiven Betrieb.

SCHRITT 4: BETRIEB

Unsere Experten unterstützen Sie beim Betrieb der jeweiligen Lösung. Wir bieten modulare Service Level Agreements (SLAs). Die Lösung kann auch im Managed Security Service betrieben werden. Dies schont intern sowohl personelle als auch finanzielle Ressourcen.

Gerne unterstützen wir Sie bei allen Fragen rund um das Thema Schutz und Verwaltung privilegierter Zugriffe auf Operational Technology (OT) und Information Technology (IT).
Fragen Sie uns!

TÜV Rheinland
Digitale Transformation & Cybersecurity
Am Grauen Stein
51105 Köln
Tel. +49 221 806-0
cybersecurity@tuv.com

www.tuv.com/iam

TÜVRheinland®
Genau. Richtig.