Hausmesse 2023

UNSER SAP SOLL SICHERER WERDEN – EIN LEITFADEN

Michael Schall

4 process
OPTIMIERTE SYSTEME

Auf einen Blick

DER REFERENT

MICHAEL SCHALL

Principal Consultant

- Network & IT Security
- Application Lifecycle Management

4 process
OPTIMIERTE SYSTEME

Die Theorie

4process
OPTIMIERTE SYSTEME

Übersicht

SECURE OPERATIONS MAP

Organization	Awareness	Security Governance	Risk Management	
Process	Regulatory Process Compliance	Data Privacy & Protection	Audit & Fraud Management	
Application	User & Identity Management	Authentication & Single Sign-On	Roles & Authorization	Custom Code Security
System	Security Hardening	Secure SAP Code	Security Monitoring & Forensics	
Environment	Network Security	Operating System & Database Security	Client Security	

Secure Operations Map

ORGANIZATION

Awareness | Security Governance | Risk Management

Awareness

- Jeder Anwender muss seinen Teil beitragen.
- Ignorieren oder Umgehen von Maßnahmen kann die ganze Landschaft gefährden.
- Sicherheitsmaßnahmen müssen anwenderfreundlich und einfach zu handhaben sein.

4 process
OPTIMIERTE SYSTEME

Secure Operations Map

ORGANIZATION

Awareness | Security Governance | Risk Management

Security Governance

- IT Security ist Management Thema
- Generelle Organisation, Handhabung & Regularien
  - Auswirkung auf Konfiguration, Integration und Betrieb der IT-Systeme

Risiko Management

- Identifizierung & Bewertung von Risiken im IT-Betrieb
- Ableitung von Maßnahmen: Eindämmung oder Behebung

4 process
OPTIMIERTE SYSTEME

Secure Operations Map

APPLICATION

User & Identity Management | Authentication & Single Sign-On | Roles & Authorization | Custom Code Security

User & Identity Management

- Definierter Prozess für Lifecycle Management von Benutzern und Berechtigungen

Authentication & Single Sign-On

- Sichere Authentifizierung von Anwendern
- Absicherung von Verbindungen zwischen Systemen

Roles & Authorizations

- Definition, Verteilung und Anpassung von Rollen und Berechtigungen

4process OPTIMIERTE SYSTEME

Secure Operations Map

APPLICATION

User & Identity Management | Authentication & Single Sign-On | Roles & Authorization | Custom Code Security

Custom Code Security

- Custom Code (Lifecycle) Management
  - Design und Entwicklung unter Sicherheitsgesichtspunkten
  - Test-, Review- und Freigabeprozesse
  - Rückbau von obsoleten Eigenentwicklungen

4process OPTIMIERTE SYSTEME

Secure Operations Map

SYSTEM

Security Hardening | Secure SAP Code | Security Monitoring & Forensics

Security Hardening

- Sichere System Einstellung und Konfiguration

Secure SAP Code

- Implementierung von Support Packages oder SAP Security Notes
- Regelmäßiger Wartungsprozess

Security Monitoring & Forensics

- Erweiterung um Reaktive Maßnahmen auf Basis von Echtzeit Überwachung
- Aufbewahrung von Logs und weiteren Informationen für spätere Analysen

4process OPTIMIERTE SYSTEME

Secure Operations Map

ENVIRONMENT

Network Security

Operating System & Database Security

Client Security

Network Security

- Netzwerksegmentierung und Firewall Konzepte

Operating System & Database Security

- Basis für sichere Plattform

Client Security

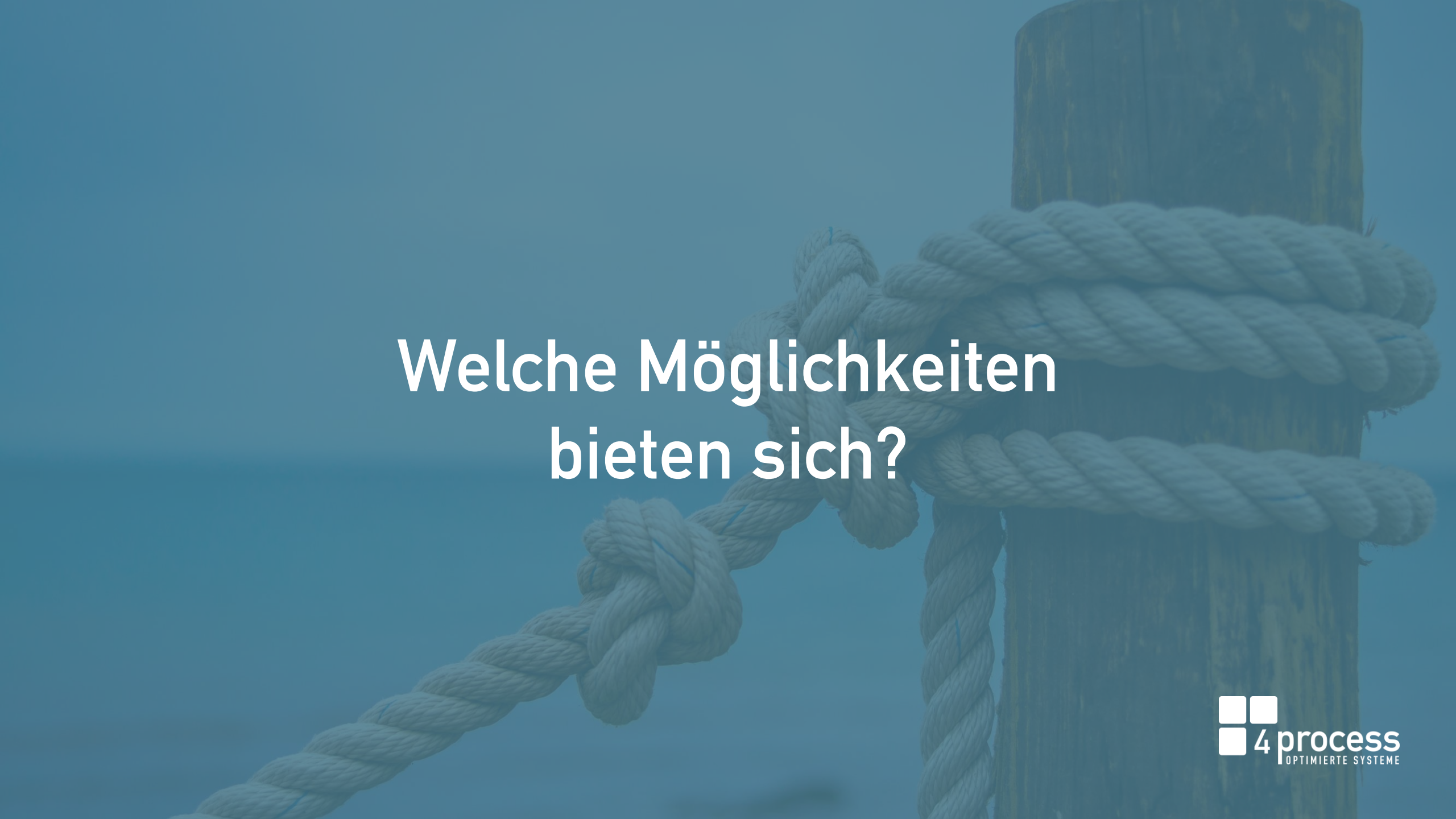
- Endgeräte Sicherheit trägt entscheiden zur Gesamtsicherheit bei

4 process
OPTIMIERTE SYSTEME

Übersicht

SECURE OPERATIONS MAP

Organization	Awareness	Security Governance	Risk Management	
Process	Regulatory Process Compliance	Data Privacy & Protection	Audit & Fraud Management	
Application	User & Identity Management	Authentication & Single Sign-On	Roles & Authorization	Custom Code Security
System	Security Hardening	Secure SAP Code	Security Monitoring & Forensics	
Environment	Network Security	Operating System & Database Security	Client Security	



Welche Möglichkeiten bieten sich?

4process
OPTIMIERTE SYSTEME

NETWORK SECURITY

Netzwerksegmentierung und Firewalls

- Trennung von Clients, Applikationsservern und Datenbanken
- Freigaben beschränken auf relevante Ports (DIAG, GW, MS, HTTP/S)
- Zugriff auf interne Ports blockieren

Environment

OPERATING SYSTEM & DATABASE SECURITY

OS-Berechtigungen

- Keine Administrator- oder Root-Rechte für SAP Service Benutzer
- Berechtigungen auf SAP System Verzeichnisse nur für SAP System Benutzer
- Strikte Berechtigungen für Verzeichnisse mit sicherheitsrelevanten Informationen

Datenbank Sicherheit

- HANA DB Hardening Guide

4 process
OPTIMIERTE SYSTEME

System

SECURITY HARDENING

SAP Security Baseline Template

- Empfehlung für ~ 120 Parameter & System/Customizing Einstellung
- ABAP, JAVA, ICM/Web Dispatcher
- Sichere Einstellungen werden zum Standard („Security by default“)
- SAP Note 2253549

4 process
OPTIMIERTE SYSTEME

System

SECURITY HARDENING

SAP Early Watch Alerts

- Umfangreiche Alerts
- Verpflichtende Übermittlung an SAP für Produktivsysteme
- SAP for Me > Systems & Provisioning > SAP EWA Workspace
- SAP Note 863362

4 process
OPTIMIERTE SYSTEME

SECURITY HARDENING - BEISPIELE

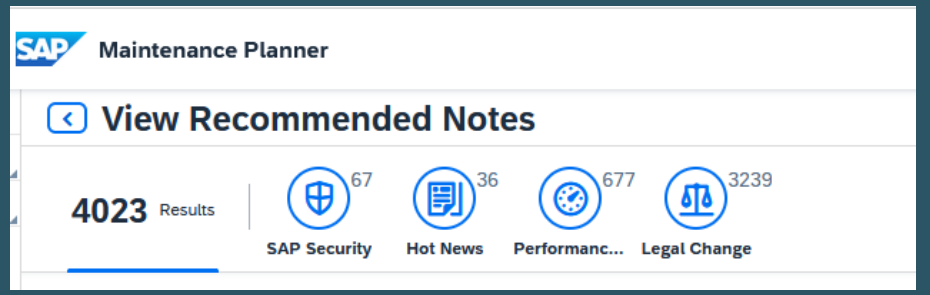
- Gateway Security
- Web Services/ICM
  - Zertifikate
  - Verifikation von Client Zertifikaten
  - Ciphersuites und weitere Parameter
- Message Server ACL & Secure Communication
- User Scripting

System

SECURE SAP CODE

SAP Security Note Recommendations

- SAP Security Notes verfügbar für Support Packages der letzten 24 Monate
- Zusätzliches Feature des SAP Maintenance Planner
- Erweiterung der SLD Data Supplier notwendig



Support Packages & Updates

- Regelmäßige Implementierung von Support Packages
- Empfehlung: einmal jährlich aktuellster SP Stack

4 process
OPTIMIERTE SYSTEME

Application

USER & IDENTITY MANAGEMENT

Zentrale Benutzerverwaltung

- Verteilung von Benutzern und Rollenzuweisungen
- System mit höchster Sicherheitsanforderung als Quelle

4process
OPTIMIERTE SYSTEME

Application

AUTHENTICATION & SINGLE SIGN-ON

Verschlüsselte Verbindungen

- SNC, HTTPS
- Gegenseitige Authentifizierung (Zertifikate)

Sichere Authentifizierung (Schnittstellen!)

- Zertifikats-basierte Authentifizierung
- OAuth 2.0
- JWT

4 process
OPTIMIERTE SYSTEME

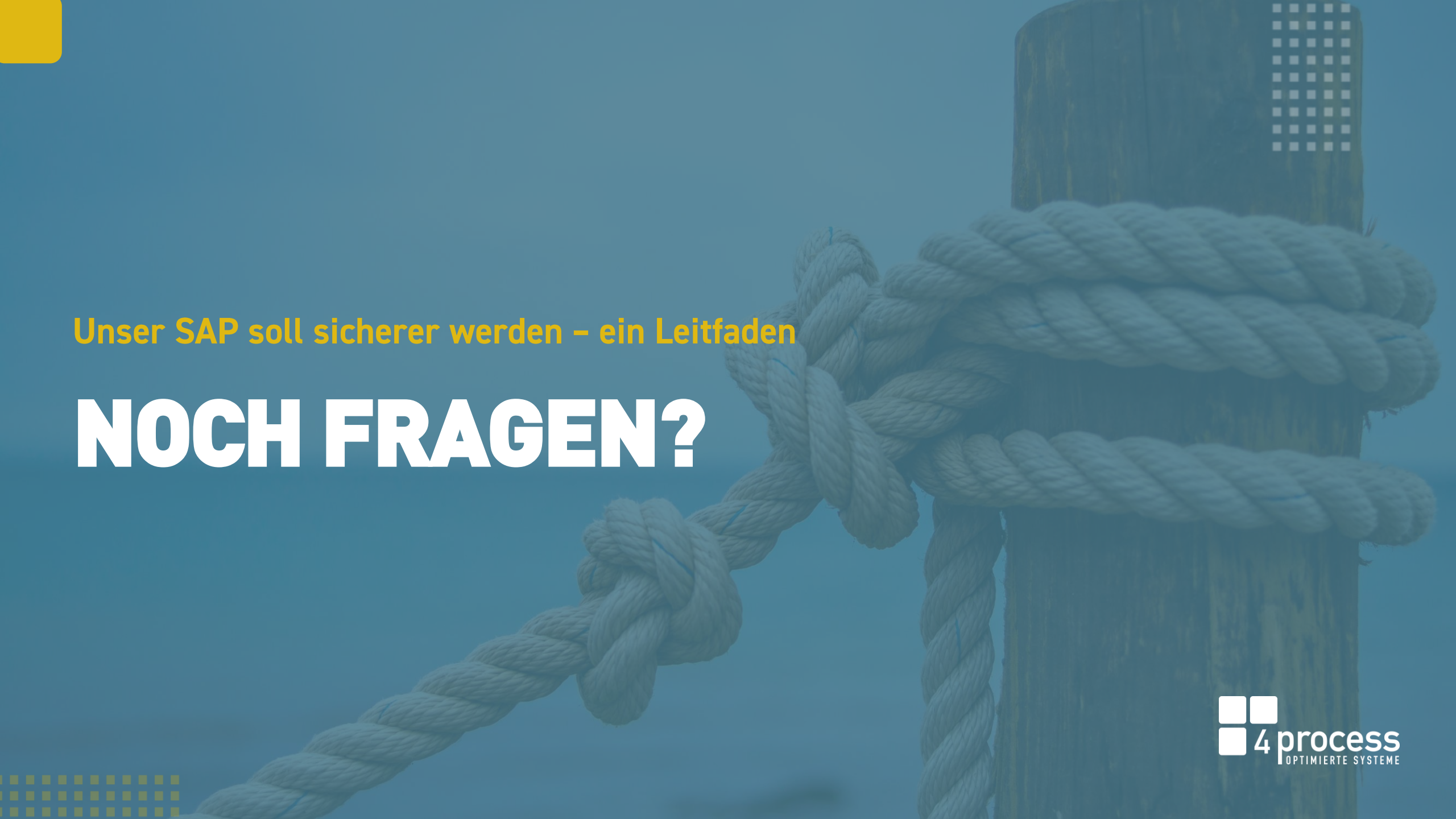
Application

AUTHENTICATION & SINGLE SIGN-ON

Single Sign-On Lösungen

- SAP GUI
  - SAP Single Single-On 3.0 (Kerberos/Zertifikate)
  - SAP Secure Login Service for SAP GUI (Kerberos/Zertifikate)
  - 4process Single Sign-On Light
- Web (Fiori)
  - SAML 2.0 / OAuth 2.0
  - Zertifikate

4process
OPTIMIERTE SYSTEME



Unser SAP soll sicherer werden – ein Leitfaden

NOCH FRAGEN?

4process
OPTIMIERTE SYSTEME

Michael Schall
B. Sc. Business Computing
Principal Consultant

4process AG
Dr.-Emil-Brichta-Straße 3a
94036 Passau

Telefon +49 851 49061-153
Telefax +49 851 49061-29
Mobil +49 151 20963176

michael.schall@4process.de
www.4process.de

4process
OPTIMIERTE SYSTEME

Vielen Dank!