**1. Einleitung**

**1.1 Ausgangssituation und Problemstellung**

**1.2 Zielsetzung der Arbeit**

**1.3 Relevanz für die All-for-One Group SE**

**1.4 Methodisches Vorgehen und Aufbau der Arbeit**

**2. Theoretische Grundlagen**

**2.1 SAP-Systemlandschaft im Überblick**

**2.1.1 SAP-Systemarchitektur (ABAP, Java, HANA etc.)**

**2.1.2 Zentrale Komponenten und Tools (z. B. SolMan, SNOTE, SPAM/SAINT)**

**2.1.3 Sicherheitsrelevante Bereiche und Module**

**2.2 SAP Security Notes – Definition und Bedeutung**

**2.2.1 Arten, Inhalte und Veröffentlichungszyklen (Patch Day)**

**2.2.2 Umsetzungsmöglichkeiten (manuell, automatisiert, Toolgestützt)**

**2.2.3 Risiken bei Nichtumsetzung (technisch, rechtlich, wirtschaftlich)**

**2.3 Grundlagen des Prozessmanagements**

**2.3.1 Geschäftsprozessmanagement im IT-Kontext**

**2.3.2 Anforderungen an sicherheitskritische Prozesse**

**2.3.3 Rollenmodelle, Verantwortlichkeiten, ITIL-Schnittstellen**

**2.4 Standards & Frameworks**

**2.4.1 ISO 27001 und BSI-Grundschutz**

**2.4.2 ITIL-Elemente (Change-, Incident-, Problem-Management)**

**2.4.3 Verknüpfung mit SAP Security Notes-Prozessen**

**3. Der ideale Standardprozess für SAP Security Notes**

**3.1 Phasenmodell eines Note-Prozesses**

**3.1.1 Erkennung und Bewertung neuer Notes**

**3.1.2 Risikoanalyse und Priorisierung**

**3.1.3 Umsetzung und technisches Patch-Handling**

**3.1.4 Dokumentation, Testing, Nachverfolgung**

**3.2 Anforderungen an einen optimierten Prozess**

**3.2.1 Effizienz, Transparenz, Nachvollziehbarkeit**

**3.2.2 Automatisierung, Kontrollmechanismen**

**3.2.3 Auditsicherheit und Rollenklarheit**

**3.3 Best Practices aus Literatur und Industrie**

**4. Ist-Analyse bei der All-for-One Group SE**

**4.1 Methodisches Vorgehen**

**4.1.1 Interviews mit relevanten Stakeholdern**

*(z. B. Marius, Micha, Tellis, Steffen, Jessi, Thomas)*

**4.1.2 Auswertung durch qualitative Inhaltsanalyse**

**4.2 Derzeitiger Umgang mit SAP Security Notes**

**4.2.1 Verantwortlichkeiten und Zuständigkeiten**

**4.2.2 Umsetzung und Dokumentation**

**4.2.3 Systemunterstützung und Tooleinsatz**

**4.3 Organisatorische und technische Hürden**

**4.3.1 Informationsflüsse und Wissenssilos**

**4.3.2 Fehlende Automatisierung und Prozessstandardisierung**

**4.3.3 Single Point of Knowledge / mangelnde Transparenz**

**4.3.4 Heterogene Systemlandschaft und technische Unterschiede**

**4.4 Kritische Schwachstellen und Risiken**

**4.4.1 Auswirkungen auf Sicherheit und Produktivität**

**4.4.2 Risikobewertung im bestehenden Ablauf**

**5. Entwicklung eines optimierten Standardprozesses**

**5.1 Zielbild und Anforderungen**

**5.1.1 Rückführung aus Analyseergebnissen**

**5.1.2 Integration organisatorischer Hürden**

**5.2 Prozessmodellierung (Soll-Zustand)**

**5.2.1 Visualisierung (z. B. BPMN)**

**5.2.2 Definition von Rollen (Service Owner, Technik, Fachbereich)**

**5.2.3 Tools, Abläufe, Entscheidungswege**

**5.3 Abgleich Ist- und Soll-Prozess**

**5.3.1 Prozessverbesserungspotenzial**

**5.3.2 Risikoreduktion und Effizienzgewinne**

**6. Theoretische Evaluation des Soll-Prozesses**

**6.1 Bewertung anhand definierter Kriterien (aus Kap. 3.2)**

**6.1.1 Sicherheit, Nachvollziehbarkeit, Umsetzungsgeschwindigkeit**

**6.1.2 Auditfähigkeit, Automatisierung, Toolintegration**

**6.2 SWOT-Analyse**

**6.3 Feedback aus Experteninterviews (Validierung)**

**7. Fazit und Ausblick**

**7.1 Zusammenfassung der Ergebnisse**

**7.2 Beantwortung der Zielsetzung**

**7.3 Grenzen der Arbeit**

**7.4 Weiterführende Empfehlungen für die All-for-One Group SE**

**8. Literaturverzeichnis**

* Fachliteratur, Standards, SAP-Quellen, Whitepaper, Interviewquellen

**9. Anhang**

* Interviewleitfäden
* Prozessdiagramme (IST & SOLL)
* Beispielhafte Security Notes
* Tabellen, Screenshots, Checklisten

MIRO Boards  
Kein Finaler Ablauf  
- Hinweis von SAP   
  
Schwachstellen Management Prozesss  
1. Wir erfahren  
2. Assestment (SAP Umfeld von 4-5 Kollegen nach dem Patchday)  
2.1 Bewerten der Notes  
2.2 Was muss gemacht werden und wie  
2.3 Empfehlung des Doings (Risikolevel)  
2.4 Wenn ewas nicht Standard ist, dann muss man win Workaraound machen  
3. Behebung

3.1 Prozess für Einspielung von Patches

Kernelpatch-> Wie kommt die Änderung ins System -> Entwicklung -> Qualiy -> Produktivb  
Kundenabsprache  
Reihenfolge  
Einspielen  
  
BusinessObejects -> Zügiger Ablauf erstellen. Schritte aufbauen damit alles schneller durchkommt