**Fragenkatalog für den betrieblichen Betreuer**

**Ziel: Erhebung des tatsächlichen Prozesses zur Umsetzung von SAP Security Notes (von Ankündigung bis Kundenrückmeldung)**

**1. Grundlegendes Verständnis**

1. Wo beginnt der Standardprozess zur Umsetzung von SAP Security Notes im Unternehmen konkret?
2. Was ist das übergeordnete Ziel dieses Prozesses – technische Sicherheit, Kundenservice, Compliance, oder eine Kombination davon?
3. Zu welchem Bereich gehört der Gesamtprozess organisatorisch – z. B. IT-Security, SAP-Basis, Service Operations, Kundenmanagement?

**2. Beteiligte Rollen und Verantwortlichkeiten**

1. Wer ist zuständig für die initiale Bewertung neuer SAP Security Notes?
2. Aus welchen Abteilungen oder Rollen besteht dieses Prüfer-Team konkret?
3. Wer trifft letztlich die Entscheidung über „relevant“ vs. „warten auf Stackupdate“?
4. Welche Rolle übernimmt das SAP-Team im Gesamtprozess – rein technisch oder auch organisatorisch (Kommunikation, Dokumentation etc.)?

**3. Prozessablauf im Detail**

1. Was passiert nach der Entscheidung, dass eine Note umgesetzt werden soll?
2. Wie werden Aufgaben dokumentiert – erfolgt die Übergabe per Ticket, Mail, Meeting?
3. Wie wird sichergestellt, dass alle Beteiligten (z. B. SAP-Team) die nötigen Informationen vollständig erhalten?
4. Gibt es eine zentrale Dokumentation oder ein Tool zur Nachverfolgung aller Notes und Umsetzungen?
5. Was passiert, wenn sich Kunden selbstständig um Notes kümmern – gibt es hier eine Eskalation oder ein Abgleichsystem?

**4. Kundenkommunikation**

1. Wer ist für die Kundeninformation zuständig, sobald klar ist, dass ein Patch durchgeführt werden muss?
2. Wie wird der Patch-Termin mit dem Kunden vereinbart – individuell oder auf Basis von Standardfenstern?
3. Wäre es denkbar, mit fixen Wartungsfenstern zu arbeiten, um den Kommunikationsaufwand zu reduzieren?

**5. Durchführung und Abschluss**

1. Wer führt die Patches technisch durch (SAP-Team?)
2. Wie wird nach erfolgreichem Patch sichergestellt, dass der Kunde informiert wird – automatisch, manuell?
3. Wird irgendwo dokumentiert, wann und wie die Note abgeschlossen wurde (z. B. zur Auditfähigkeit)?

**6. Schwachstellen und Verbesserungspotenzial**

1. An welchen Stellen im Ablauf gehen aktuell Informationen verloren?
2. Welche Schritte könnten deiner Einschätzung nach automatisiert oder durch ein Tool besser unterstützt werden?
3. Gibt es bereits Ideen oder Pilotprojekte zur Prozessverbesserung?

**7. Individuelle Einschätzung**

1. Wie schätzen Sie den aktuellen Prozess in Bezug auf Effizienz, Transparenz und Sicherheit ein?
2. Was sind aus Ihrer Sicht die größten Risiken im derzeitigen Ablauf?
3. Gibt es aus Ihrer Erfahrung wiederkehrende Probleme oder typische Konfliktstellen?

**🔍 A. Allgemeiner Ablauf & Verantwortlichkeiten**

1. **Wo beginnt bei uns im Unternehmen der Prozess zur Bearbeitung von SAP Security Notes?  
   → Wer ist initial verantwortlich für die Sichtung und Bewertung?**
2. **Welche Abteilungen oder Rollen sind im Gesamtprozess involviert?  
   → Von der Bewertung bis zur Durchführung und Rückmeldung an Kunden**
3. **Welche Rolle übernimmt das SAP-Team im Gesamtprozess?  
   → Nur technische Umsetzung oder auch Kommunikation, Bewertung, Dokumentation?**
4. **Wird der Ablauf einheitlich für alle Kundenprojekte angewendet oder hängt das vom jeweiligen Projekt / Team ab?**

**🧠 B. Entscheidungsfindung & Bewertung**

1. **Wie läuft die Entscheidung ab, ob eine SAP Security Note umgesetzt wird oder nicht?  
   → Gibt es feste Kriterien, oder ist das abhängig vom Einzelfall?**
2. **Gab es in der Vergangenheit konkrete Vorfälle (z. B. Sicherheitsprobleme), weil Notes zu spät oder nicht umgesetzt wurden?**
3. **Gab es bereits Versuche, einen einheitlichen Prozess zu etablieren?  
   → Wenn ja: Warum hat es bisher nicht geklappt?**

**📊 C. Steuerung, Tools & Dokumentation**

1. **Wie wird die Umsetzung einer Note intern organisiert und dokumentiert?  
   → Gibt es zentrale Tools (z. B. Jira, ServiceNow) oder läuft das über E-Mails, Tickets, Meetings?**
2. **Gibt es eine zentrale Übersicht, welche Notes wann und wie umgesetzt wurden?  
   → Oder ist das personenabhängig und dezentral organisiert?**
3. **Wird die durchschnittliche Durchlaufzeit einer Note gemessen?  
   → Wie lange dauert es typischerweise von Veröffentlichung bis Umsetzung?  
   → Gibt es Unterschiede je nach Kritikalität (z. B. „Hot News“)?  
   → Was sind typische Verzögerungsfaktoren?**

**📬 D. Kundenkommunikation & Transparenz**

1. **Wie wird der Kunde in den Prozess eingebunden?  
   → Wer informiert den Kunden?  
   → Wie wird ein Termin vereinbart?  
   → Wie erfolgt die Rückmeldung nach erfolgreichem Patch?**
2. **Gibt es einen standardisierten Kommunikationsweg (z. B. über ein Ticketsystem)?**

**⚠️ E. Probleme & Optimierungspotenzial**

1. **Wo im aktuellen Prozess gehen regelmäßig Informationen verloren oder kommt es zu Missverständnissen?**
2. **Welche Verbesserungsideen oder Automatisierungsmöglichkeiten sehen Sie?  
   → Z. B. zentrale Steuerung, feste Wartungsfenster, einheitliche Tools, automatisierte Erkennung & Bewertung**
3. **Welche Rolle spielen SAP Security Notes bei internen oder externen Audits (z. B. ISO 27001)?  
   → Gibt es Anforderungen an Nachweise, Protokolle oder Fristen?**

Mögliche Problembereiche:

* Sicherheitslücken bleiben unentdeckt oder ungeschützt
* Informationen werden per Mail, Word-Doku, Ticketsystem parallel verteilt
* Fehlende zentrale Übersicht zu offenen, abgeschlossenen oder nicht umgesetzten Notes
* Keine konsistente Nachverfolgung möglich
* Kein geregelter Rhythmus → Notes werden „nebenbei“ behandelt
* Verzögerte Kundenkommunikation und Patch-Termine
* Fehlerhafte oder lückenhafte Dokumentation der Note-Umsetzung

Involvierte TEAMS:  
SCO  
ITNA (nimmt nur etwas Arbeit ab)  
2nd\_lvl\_SAP

Problempunkte lt. Ali

1. Infos von Thomas Team bei SAP-News werden zwar Kunden vermittelt aber SAP-TEAM wird außen vorgelassen
   1. SOC – Security Operation Center
2. Es gibt keinen Prozess der alle beteiligten Abteilungen einschließt
3. Changeformular?
4. Zeitfrage schwer zu beantworten, da unterschiedliche Themen
5. Kunden werden teilweise doppelt informiert (Es gibt keine Liveliste)

Wichtig:

Organisatorisch  
Informationsfluss  
Schwachstellen Theoretisch

Wir haben das Problem, dass innerhalb der Abwicklung von Patches/Notes/Hot News einige Lücken exestieren.  
Wenn SAP News veröffentlicht, dann werden diese von SOC-Team bearbeitet und eingestuft. Wir haben als Dienstleister eine Meldepflicht. Bedeutet, dass alle Kunden über diese News informiert werden, ob kritisch oder nicht spielt hier keine Rolle.  
Sind news kritisch und ein Handeln ist notwenig, dann werden die Kunden informiert und es werden Tickets über ITNA erstellt und in der Queue von 2nd\_lvl\_sap eingespielt.  
Problem hier ist, dass bis dahin keine Infos an 2ndlvlsap weitergetragen wurden. Teilweise werden wir dann von den Kunden informiert. Desweiteren besteht für das SAP\_TEAM keine Reaktionszeit in der sie sich vorbereiten können.  
ebenso exestiert keine Übersicht bei welchem Kunden schon was gemacht wurde, daher passiert es auch, dass Tickets gar nicht mehr bearbeitet werden müssen aber wir als Firma das nicht erfahren.

TO-DO

1. Mit Thomaß nach Ablauf sprechen wie es im SOC Team genau abläuft
   1. Prozess vom SOC-TEAM aufstellen und Schwachstellen finden
   2. Kommunikationsablauf herausfinden
   3. Verbesserungsvorschläge

Patching ist nicht immer Inbegriffen und werden von den Servicemanager (BGS\_SEM\_GBS) bezüglich Kosten geregelt.

Messbare Werte:  
- Kundenzufriedenheit  
- Zeitersparnis  
>