BAUMGUARD
Let no one else be /root

Compliance per „Knopfdruck“

Mit modernem ITSM bereit für NIS-2 oder ISO27001

SECTORNORDAG
OpenSource based enterprise solutions

ITSM-SUMMIT 2026

Referent

Benjamin Büttelmann

Freiberuflicher IT-Consultant, Auditor, Dozent und Geschäftsführer baumguard OHG

Werdegang

- Diplomstudiengang Informatik in Bremen
- 16 Jahre IT-Beratung und Projektleitung zur Einführung und Optimierung von ITSM (speziell nach ITIL) und ISMS (spe ISO27001 und TISAX)
- Seit 2025 als Dozent für Informationssicherheitsthemen
- Seit Anfang 2026akkr. Lead Auditor für ISO27001
- Seit 7 Jahren Partner der SECTOR NORD AG

Ausgangssituation

- ISO/IEC 27001 Audit steht kurz bevor
- Geschäftsführung ist der Überzeugung „IT kümmert sich“
- IT stellt überrascht fest, schon wieder Audit, war nicht gerade erst eins?
- Daraufhin wird panisch das Tagesgeschäft eingestellt
- ISB (wenn vorhanden) überlegt, was alles benötigt wird
- Risikomanagement wurde wieder nicht aktualisiert
- Dokumente werden nicht gefunden
- Die letzten Excel-Tabellen werden manipuliert …ähm gepflegt
- Na gut, „Mut zur Lücke“…

Ergebnis

Kein geeignetes, wirksames und angemessenes ISMS vorhanden!

Was sind die Probleme?

„IT kümmert sich schon…“

- Geschäftsführung kommt Ihrer Verantwortung nicht nach
- Informationssicherheit wird mit IT-Sicherheit gleichgesetzt
- Anforderungssituation ist unklar (Fehlendes Verständnis)

Ressourcen, Qualität und Zeit

- Projekte werden parallel zum Tagesgeschäft „nebenbei“ verrichtet
- Dokumente werden (KI-generiert) einmalig erstellt, aber nicht gelebt
- Heterogene IT-Systemlandschaft (ITSM, GRC, CRM, ERP, BPM, BCM,..)

BAUM GUARD
Let no one else be /root

Was sagt die Compliance? (1v2)

Das fordert ISO/IEC 27001

- Verpflichtung der obersten Leitung zur erfolgreichen Umsetzung des ISMS
- Die Organisation muss ein ISMS aufbauen, verwirklichen, aufrechterhalten und fortlaufend verbessern
- Es sind organisatorische, personelle, physische und technische Maßnahmen umzusetzen
- Maßnahmen müssen angemessen, geeignet und wirksam sein

BAUM GUARD
Let no one else be /root

Was sagt die Compliance? (2v2)

NIS2 verlangt

- Geschäftsführung haften persönlich für fahrlässig verursachte Sicherheitsvorfälle
- Pflichten sind nicht delegierbar
- 10 Mindestmaßnahmen für das Risikomanagement (geeignet, wirksam und verhältnismäßig)
- Umsetzung von Maßnahmen nach Stand der Technik

Konsolidierung

BAUM GUARD
Let no one else be /root

Geschäftsprozessmgmt

NIS-2

- 10 Mindestmaßnahmen
- Persönlich Haftung
- Meldepflicht ans BSI
- Business Continuity

ISO27001

- ToMs am nach Stand-der-Technik
- PDCA-Zyklus
- Klare Governance
- Kontinuierliche Verbesserung

Risikomanagement

Compliance, aber

…was hat IT-Servicemanagement jetzt damit zu tun?

ITSM als Fundament

BAUMGUARD
Let no one else be /root

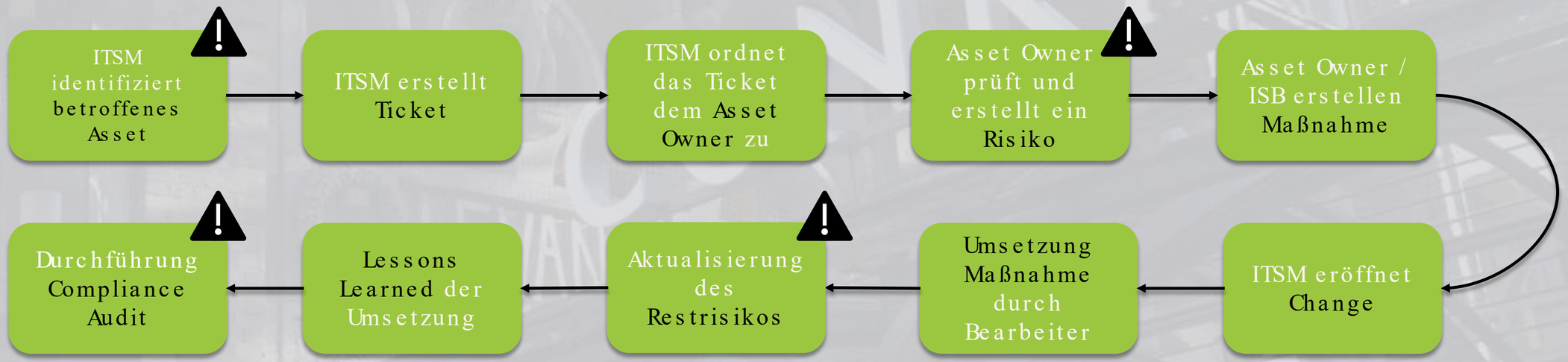
Das kann ITSM (u.a.)

- **CMDB** als Assetbasis zur **Risikobewertung und Schutzbedarfsfeststellung**
- Verwaltung von **Geschäftsprozessen** als Assets
- Integration und Zuordnung von **Controls** zu Assets, die als Maßnahmen im ITSM vorhanden sind
- (**Security**) **Incident** Management und automatisierte Meldung ans BSI, LDSB, …
- **Lieferanten-** und Lizenzmanagement
- **Change Management** inkl. **Lessons Learned** zur Durchsetzung von Änderungen an Tech und Managementsystem bzw. Geschäftsprozessen (**Risikomanagement**)
- **IAM** als automatisierter Prozess für das Berechtigungsmanagement
- **Threat Management** zur frühzeitigen Erkennung von Schwachstellen und Netzwerkanomalien

BAUMGUARD
Let no one else be /root

Szenario

Eine Schwachstelle wurde identifiziert…



BAUMGUARD
Let no one else be /root

ITSM enabled Compliance

- **Identifizierung** und **Zuordnung** einer **Schwachstelle** zur IT UND dem korrespondierenden **Geschäftsprozess** durch hierarchische Beziehungen innerhalb der **CMDB**
- Bewertung ob **Sicherheitsvorfall** oder **Sicherheitsereignis**
- Wissen über die relevanten **Stakeholder** zur weiteren Abarbeitung bzw. **Informierung** (bspw. BSI-Meldung)
- Bewertung der **Priorität** bzw. **Kritikalität** durch vorige **Schutzbedarfsfeststellung**
- **SLA**-Monitoring / **KPI**-Monitoring in Form von Dashboards
- Kontinuierlicher Verbesserungsprozess (**KVP**)
- **Brutto-/ Nettorisikobetrachtung** und Bewertung
- **Wirksamkeitsbewertung** (durch SLA, Audit, ..) der umgesetzten Maßnahmen

Erfolgsfaktoren (lv2)

Erhöung der Datenqualität

- „Shit-in-Shit-out“
- Einsatz einer gepflegten zentralen CMDB (alle Informations-Assets)

Aufbrechen von „Silos“

- Funktionen müssen zu Prozessen zusammengefasst werden
- Integration von Services und Prozesse in einem Tool
- Nutzung von Self-Service-Portalen

„Harmonisches“ Tooling

- Geeigneter Tooleinsatz (auf Grundlage der Anforderungssituation)

BAUMGUARD
Let no one else be /root

Erfolgsfaktoren (2v2)

Management Commitment

- Vorbildfunktion
- Bereitstellung ausreichender und angemessener Ressourcen

Kultureller Wandel

- Informationssicherheit muss integraler Bestandteil von Prozesse werden
- Prozesse dürfen sich nicht schwergewichtig anfühlen

„Betroffene zu Beteiligten machen“

- Frühstmögliche Mitnahme der Mitarbeiter
- Toyota Modell

BAUMGUARD
Let no one else be /root

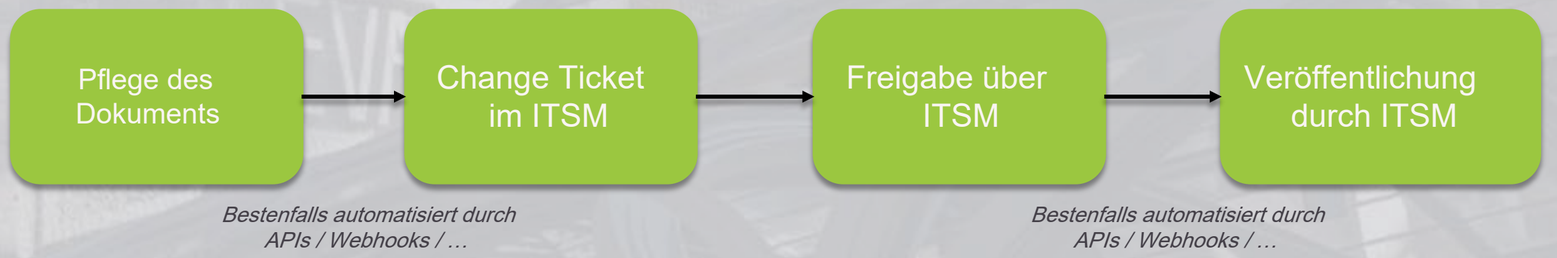
Was ist mit Dokumentation?

- Eine der größten Schwachstellen von ITSM-Lösungen
- Eine Pflege der ISMS-Dokumentation innerhalb von ITSM-Tools ist nicht empfehlenswert
- Tools zur Pflege von Dokumenten oder Wissen sind weit verbreitet und vor allem tief im Unternehmen verwurzelt
- Was ist also die Antwort auf die Frage…

Wie integriere ich die Dokumentation ins ITSM?

Dokumente als Assets

- Aufnahme der Dokumente als Assets in der CMDB (per Verlinkung)
- Wichtig hierbei ist eine klare Trennung zwischen der eigentlichen Pflege, Verteilung und Freigabe
- Die Pflege und Bearbeitung der Dokumente erfolgt im dafür vorgesehenen Tool
- Da es sich weitgehend um strategische Dokumente handelt, die den SOLL-Stand beschreiben, sollten sie mit den zugehörigen Daten aus dem ITSM verknüpft werden (Bspw. als Anhang)



BAUMGUARD
Let no one else be /root

Zusammenfassung

Continuous Compliance

- Compliance darf keine jährliche „Sonderaufgabe“ sein, sondern muss als kontinuierlicher, integrativer Prozess im Managementsystem gelebt werden

Kulturwandel

- Geschäftsführung und Belegschaft müssen ISMS als Enabler begreifen, nicht als bürokratische Hürde

Synergien nutzen

- Vorhandene ITSM-Tools bieten bereits ein gutes Fundament, um NIS-2 oder ISO 27001 umzusetzen

Mensch & Prozess vor Tool

- Organisation und Prozesse sind der Schlüssel, die Technologie ist der Enabler.

Erstes Fazit

BAUM GUARD
Let no one else be /root

Die Lösung für den 'Knopfdruck' ist kein monolithisches Tool, sondern eine intelligente Verknüpfung von ISMS und ITSM.

BAUMGUARD
Let no one else be /root

Aussicht

Einsatz von KI

- KI kann die zuvor genannte Synergie von ITSM und ISMS sowie Dokumente weiter vertiefen
- Die KI könnte tatsächlich das Audit komplett selbst durchführen inkl. der Nachweiserbringung bzw. Nachweisgenerierung
- „Predictive Compliance“ zur Verknüpfung historischer Daten mit externen Threat Intelligence Daten
- Verknüpfung von ITSM und ISMS erleichtert die Erfüllung des EU AI Act
- KI-Anwendungen müssen zukünftig ebenfalls als Asset in der CMDB gepflegt werden

Schlussfazit

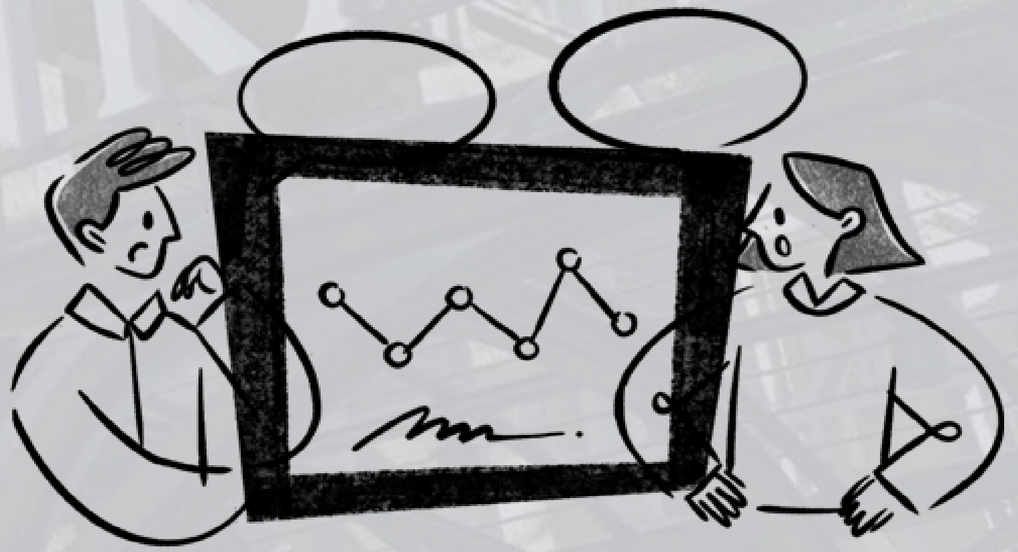
BAUM GUARD
Let no one else be /root

Wer also heute noch in Excel-Tabellen feststeckt, steht immer wieder vor denselben Herausforderungen innerhalb seine ISMS und verpasst zudem den Anschluss an die KI-gestützte Cybersicherheit.

BAUMGUARD
Let no one else be /root

VielenDank!

Gibt es Fragen?



BenjaminBüttelmann
Geschäftsführer baumguard OHG
(0170) 9639089
bb@baumguard.de
www.baumguard.de