AEB

Erfahrungsbericht zum Betrieb des ISMS bei AEB

Warum wir im ISMS was wie machen …

Volkher Wegst (ISMS Manager bei AEB)

Gliederung

1

Kurze Vorstellung Referent und Firma AEB

2

Warum setzt AEB auf ISMS und ISO 27001?

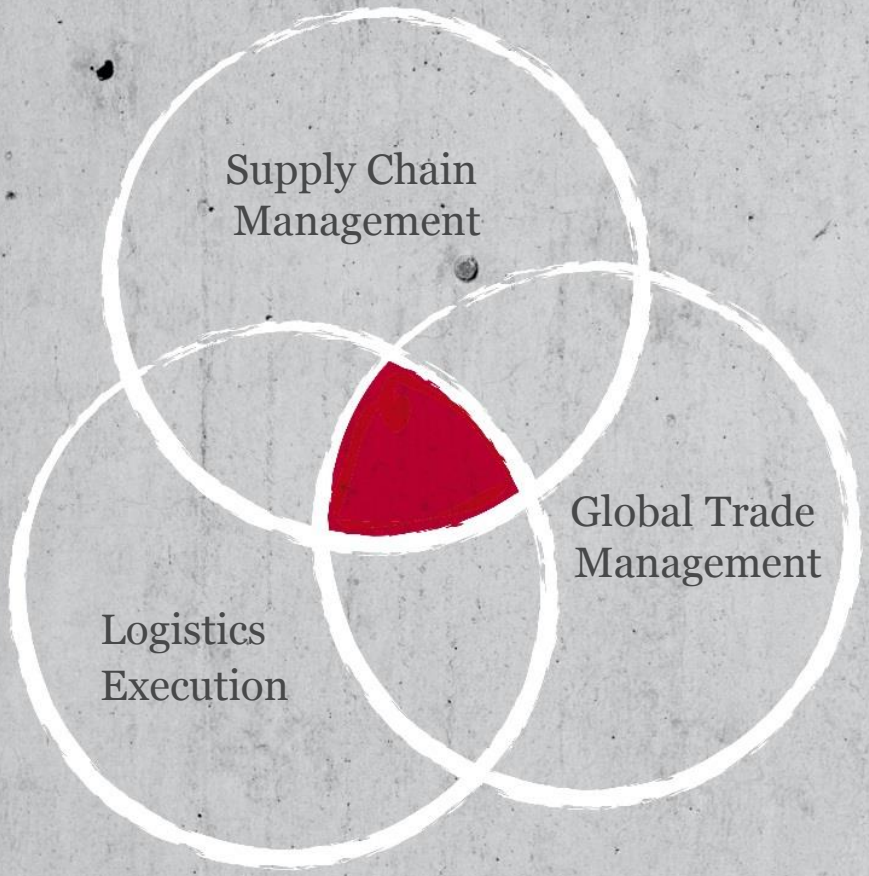
3

Was erlebe ich als besonders?

4

FAZIT / Mein Credo als ISMS Manager

AEB: Partner auf der ganzen Welt



5000+ Kunden

15 Standorte, 9 Länder

400+ Mitarbeiter

Gegründet 1979

ASSIST4 – SCM-Lösungen im Überblick

Visibility & Collaboration Platform

Die Basis für effiziente Zusammenarbeit in der Supply Chain. Transparenz und Performance. End-to-end.

Order Management

Ordnung in Ihren Bestellprozessen. Übersicht über Ihr Fulfillment. Kontrolle über die Kosten und Abläufe.

Warehouse Management

Unterstützung aller Prozesse im Lager oder Distributionszentrum. Wirtschaftliche Gestaltung Ihrer Lagerabläufe.

Transport & Freight Management

Robuste Prozesse in der Supply Chain Execution: Transportabwicklung und Frachtkosten im Griff.

Customs Management

Business Services für alle Zollprozesse in Beschaffung und Distribution. Standardisiert. Automatisiert. Integriert.

Compliance & Risk Management

Absicherung Ihrer Prozesse gegen Risiken. Vermeidung von Verstößen gegen Vorschriften. Sicheres Handeln.

Vorstellung des Referenten

- Volkher Wegst
- Seit 2001 bei AEB (am Standort Stuttgart) tätig
- Seit 2009:
  - Bestellter betrieblicher Datenschutzbeauftragter
  - ISMS Manager (seit Einführung des ISMS)
  - Notfallbeauftragter (Stichwort BCM)
- Seit 2014: Kunde/“Partner“ der SerNet; Einsatz von Verinice.PRO

Warum setzt AEB auf ISMS/ISO 27001? -1-

- AEB ist IT-Provider mit eigenem Hosting -> Cloud
- Vertrauensbildung endet nicht beim Angebot guter Produkte….diese müssen auch zuverlässig im Betrieb sein; Tag für Tag stehen wir in dieser Pflicht.
- Dazu gehört auch das Signal, dass wir den Blick werfen auf „Was wäre, wenn …..“
  - meint also das Risikomanagement
  - und auch Business Continuity Management
  - mit unseren Services vereinbaren wir Service Level Agreements (Standard und ggf. sonder-vereinbarte SLA); auch dort ist Verfügbarkeit ein Thema
- … dies interessiert unsere Kunden wirklich (und zunehmend)

Warum setzt AEB auf ISMS/ISO 27001? -2-

- Wir nehmen Datenschutz ernst; mit der kommenden EU-Datenschutz-Grundverordnung werden einige Themen noch ernster werden
  - unsere Kunden als verantwortliche Stelle + AEB als Auftragsverarbeiter treten als **gemeinsam Verantwortliche** auf
  - beide Beteiligte sind aufgerufen, eine **Datenschutz-Folgenabschätzung** abzugeben -> da sind wir schnell beim Risikomanagement…beginnend mit der Einschätzung des Schutzbedarfs von Daten und ihrem Einsatz und der nachvollziehbaren Bewertung eines angemessenen Schutzes

- Bei AEB ist dieser Blick also nicht nur nach innen gerichtet, sondern betrifft die Zuverlässigkeit für unsere Kunden bzgl. Verfügbarkeit und Vertraulichkeit (und Integrität). Zur tatsächlichen und nicht „nur“ juristischen Absicherung.

- Daher setzen wir ISMS als ständigen Prozess ein. Was heißt das? Dazu kommen wir beim übernächsten Punkt…

Warum setzt AEB Verinice.PRO ein?

- Wir wollten ein **intuitive**s Werkzeug mit guter **Usability**
- … mit der Möglichkeit, die Aufgaben zum Betrieb auf mehrere Schultern (eine je Domäne) zu legen; daher haben wir unsere Bereiche (Domänen) als Organisationseinheit angelegt. Nicht Standorte. Die Domänen haben bei uns den Blick auf die Sache, nicht auf Linien-Organisation.
- Für Mitarbeiter, für die der Umgang mit ISMS und die Bedienung eines Risiko-Tools immer noch einen vergleichsweise niedrigen Anteil (<10%) ihrer Ressource einnimmt. Wichtiger war uns, dass das **fachliche, organisatorische und … ISMS-intellektuelle Verständnis je Domäne in 1 Hand** liegt.
- Als Schwaben durfte es uns auch nicht ganz teuer sein, sondern eben … preiswert

Was erlebe ich als besonders? – 1.7 -

- Unsere organisatorische Umsetzung

2 Zusammensetzung des IS-Boards

... in Maximalausprägung:

- ein Vertreter der Geschäftsführung (nicht ständig)
- Leitung ISB: ISMS-Leitung
- Rolle: Domänen Sicherheitsbeauftragter (**Zyklus für Termine** für Risikobewertung und -behandlung) wie folgt:

Rolle in	Zyklus für Termine
Services ( ); ggf. mit mwu, dm, vw)	(2 Monate)
IT ( ); ggf. mit Michae er)	(2 Monate)
Verwaltung (r); ggf. mit vw)	(3 Monate)
Vertrieb/Vermarktung ( ), vertreten durch Domänen-Sicherheitsbeauftragter: er)	(3 Monate)
Lösungen (Yvonn)	(3 Monate)
Produkte (er)	(3 Monate)

- ggf. Auditor/Auditorin für internes Audit

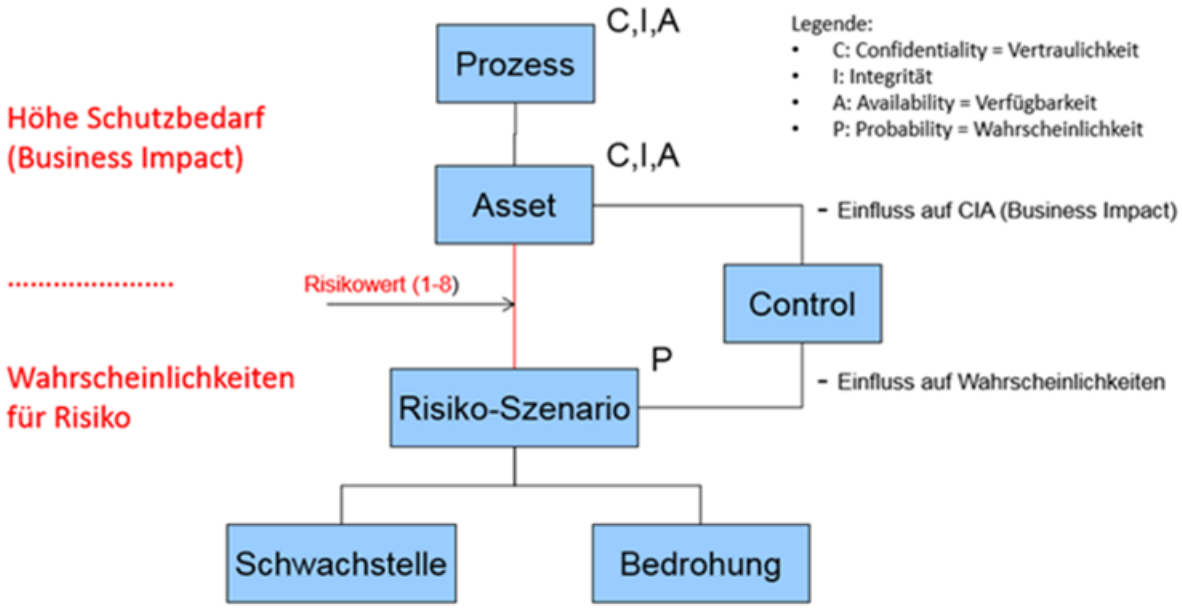
Was erlebe ich als besonders? – 2.7 -

- Sehr intensiver Betrieb des ISMS
  - häufige Sitzungen zwischen dem ISMS-Manager und den so genannten Domänen-Sicherheitsbeauftragten (alle 1-2 Monate spätestens)
  - Managementbewertung quartalsweise 4+1 je Jahr; je ca. 1 Stunde mit GL und ISMS-Leitung; ca. 2-3 Seiten Doku zum Rückblick und Einschätzungen; Anlass für Neubewertung und Abstimmung zur Risikobehandlung

- Unsere Überlegungen zur Risikobehandlung sind wenigstens gleichrangig wie die Überlegungen zur Risikoeinschätzung. **Unser Interesse richtet sich daher immer auf die Verknüpfung von asset und Szenario**. Jede Kombination ist eine andere Situation, die
  - zu bestimmten Risikowerten führt
  - damit auch gesondert dort (!) zu betrachten ist, welche Option der Risikobehandlung zu entscheiden ist (Akzeptanz, Vermeiden, Reduzieren …)
  - daher macht die AEB dies dort und hat in Verinice hierfür bisher das Feld „Beschreibung“ genutzt. -> nun neue Combo-Box seit Verinice 1.13.1

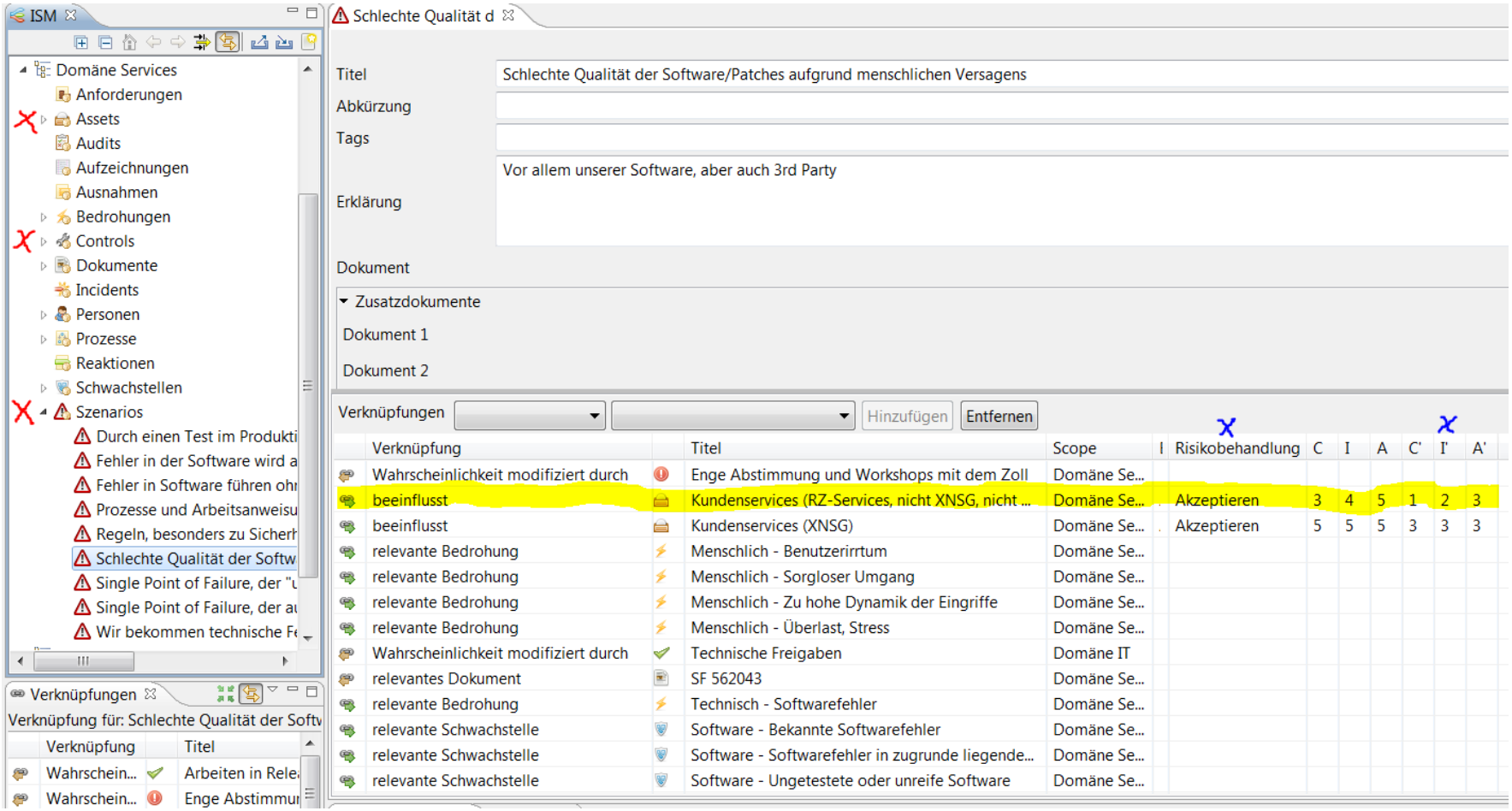
Was erlebe ich als besonders? – 3.7 -

- Anders gesagt: Nein, wir stellen die Gedanken zur Risikobehandlung (samt Entscheidung) bewusst nicht im asset an. Weil wir das vom Datenmodell her und in der Sache für verkehrt halten.



Diese Ansicht ist übrigens eine Seite unserer Risikokarte, die den Kollegen immer wieder zur Einordnung hilft.

Was erlebe ich als besonders? – 4.7 -



Was erlebe ich als besonders? – 5.7 -

- Wir bringen dieses Ergebnis auch im Report zum Ausdruck:

Szenario	Asset	BCM relevant	Erklärung Szenario	Erklärung Asset	Erklärung Verknüpfung	Betrifft Vertraulichkeit	Betrifft Integrität	Betrifft Verfügbarkeit	Bedrohung shäufigkeit	MAX: Risikobewertung mit vorhanden Controls
(Empfindliche) Hardware, die aus Versehen bedroht wird	Kritische Sicherheitseinrichtungen	Nein		Auch Tools wier z.B. Hostmon oder RRD Tool	Akzeptanz	Nein	Ja	Ja	1	4
Durch einen Test im Produktivsystem kommt es zu Problemen oder gar zu einem Emergency	Applikationsserver	Nein			Akzeptanz	Nein	Ja	Ja	0	2
Durch einen Test im Produktivsystem kommt es zu Problemen oder gar zu einem Emergency	Back-Up-System	Nein			Akzeptanz	Nein	Ja	Ja	0	2
Durch einen Test im Produktivsystem kommt es zu Problemen oder gar zu einem Emergency	DB Archive Logs	Nein			Reduzieren	Nein	Ja	Ja	0	3
Durch einen Test im Produktivsystem kommt es zu Problemen oder gar zu einem Emergency	DB Server	Nein			Reduzieren	Nein	Ja	Ja	0	2
Durch einen Test im Produktivsystem kommt es zu Problemen oder gar zu einem Emergency	Kritische Anwendung (Intern)	Nein			Akzeptanz	Nein	Ja	Ja	0	2
Durch einen Test im Produktivsystem kommt es zu Problemen oder gar zu einem Emergency	Kritische RZ Hardware	Nein			Reduzieren	Nein	Ja	Ja	0	2
Durch einen Test im Produktivsystem kommt es zu Problemen oder gar zu einem	Kundendat	Nein			Reduzieren	Nein	Ja	Ja	0	3

Report

Was erlebe ich als besonders? – 6.7 -

- Erst in der Verknüpfung aus dem (hier ein und demselben) Szenario mit dem asset entsteht das Risiko. Erst für die Kombination kann ich sagen, ob ich das akzeptiere oder etwas dagegen unternehmen möchte. Ich akzeptiere ja nicht das asset oder das Szenario, sondern die kombinierte Situation aus asset und Szenario. -> eingeflossen in der Version 1.13.1. Und: User wollen ihre Ergebnisse direkt in Verinice sehen.

- Bedenken zur Daten-Modellierung? -> Einige AEB-ISMS-Statistik-Daten:
  - 8 Organisationseinheiten; mit je eigener Zuständigkeit (Rolle: Domänen-Sicherheitsbeauftragter)
  - 5 - 50 assets je Organisationseinheit
  - 5 - 20 Szenarios je Organisationseinheit

- Nein: wir haben nicht im worst-case 20*50=1000 Kombis; sondern „in echt“: < 100. Mit entsprechender Selektion (im Excel-Report bequem möglich) konzentriert sich die Arbeit dann auf etwa 60 Datensätze, mit ca. 10 Szenarios.

Was erlebe ich als besonders? – 7.7 -

- An der Stelle der Controls machen wir einen Medien-“Bruch“; wir wechseln in unser Incident-Management-System
  - Mit dem Charme, diese Incidents auch weiteren Kollegen zur Bearbeitung/Untersuchung weiter zu dispatchen, die bewusst keinen Zugang zu Verinice.PRO haben
  - Es gibt aber eine Kreuz-Referenz zwischen Controls und Incidents so, dass der Anwender navigieren kann zu „wie geht es mit den Gegen-Maßnahmen weiter?“.
  - Controls sind aus unserer Sicht dann die wirklich kreative Arbeit …
  - Die Verinice-Klasse „Dokumente“ verwenden wir dann gerne für
    - obige Incidents als Belege
    - Richtlinien, Anweisungen, Anleitungen …. (also eher organisator. Controls-Anlagen), z.B. sind das WIKI-Seiten in unserem Intranet

FAZIT: Mein Credo als ISMS-Manager - 1 -

- **1. Gute Datenmodellierung!!**
  - Die Datenmodellierung selbst kann ein Lern-Prozess sein, wo man iterativ die Dinge mal näher detaillieren muss, mal generischer ausprägen darf.
  - Es muss eben nicht (!) einheitlich homogen detailliert sein.
  - In einer späteren Phase kann man auch schauen, ob man Dinge wieder „vor die Klammer ziehen kann“. Beispiel: Controls, die auf viele assets auch unterschiedlicher Organisationseinheiten wirken.

- **2. Akzeptanz der Mitarbeiter** (insbesondere Key-User) ist sehr wichtig
  - Ja, sie haben Zusatzarbeiten
  - ISMS ist für sie kein Full-time-job; das würden sie auch nicht wollen …
  - Im persönlichen (!) Gespräch abstimmen, wie häufig man sich treffen mag (schwankt bei uns zwischen monatlich und 3-monatlich), wo der Schuh drückt (kann mal Ressourcen-Situation sein oder noch Defizite im Verständnis im Risikomanagement …)

FAZIT: Mein Credo als ISMS-Manager - 2 -

- **3. Organisation / Management**
  - Ja, es braucht den **Willen** von oben (samt auch Verständnis und Freigabe von Ressourcen)
  - Ja, es braucht den **Macher**, der den Betrieb des ISMS verantwortlich am Leben hält -> bei AEB: Rolle des ISMS-Managers (ca. 25%); da braucht es etwas Glück (Betriebszugehörigkeit, einiges Grundverständnis und eine organisator. Vernetzung im Bereich Security, Affinität zur Abstraktion und regelbasierter Arbeitsweise, Akzeptanz, Durchsetzungsvermögen, Fähigkeit, auch im Stillen zu arbeiten …)
  - Es braucht die **Mitstreiter**, die den Sinn auch für sich erkennen und in ISMS einfließen lassen bzw. aus ISMS Aktivitäten ableiten
  - Es braucht auch ein **Tool für Wissensmanagement**, in dem Sie gut vernetzt/navigierbar und einfach aktualisierbar und global verfügbar z.B. Anleitungen zur Verfügung stellen können. -> bei uns WIKI -> z.B. https://wiki.pmbelz.de/w/Rolle:Domänen-Sicherheitsbeauftragter oder z.B. zu Controls samt Zuordnung, wer zuständig ist.

This is the end …?

- Über einen regen Austausch würde ich mich sehr freuen
- Ihre Fragen …
- Unsere Wünsche noch …
  - Brauchbares Dashboard direkt in Verinice, ohne Umweg über Reports
  - Tracking von Veränderungen (warum hat wann wer was zuletzt geändert)
  - Vererbung -> etwa bei Verknüpfung mit asset-Gruppen
  - Verhalten von Drag&Drop (nicht nur verknüpfen, sondern verschieben)

Vielen Dank für Ihre Aufmerksamkeit