STORYCARD · TEIL 6 · ISMS · SPRINT 6 · TRACK A UND B

Wie bleibt der Hub auch nächstes Jahr sicher?

Fünf Teile lang habt ihr für HLG Schutzbedarf festgestellt, gesichert, getestet und Maßnahmen umgesetzt. Jetzt geht es um die Frage, die jede Geschäftsleitung am Ende stellt: Was passiert, wenn ihr weg seid? In Teil 6 baut ihr das Managementsystem, das die Sicherheit des Hubs am Laufen hält, und übergebt euer Sicherheitskonzept.

Sprint 6 | **20 Stunden** | **10 CP** | **Lernangebot 17 und 18** | **Meilenstein M4**

Als Sicherheitsteam von Querwind **wollen wir** für HLG eine Leitlinie, feste Rollen und einen ISMS-Fahrplan über zwölf Monate entwerfen, unsere Maßnahmen aus Teil 1 bis 5 mit IT-Grundschutz und ISO/IEC 27001 abgleichen und alles als Sicherheitskonzept im Fachgespräch an die Geschäftsleitung übergeben, **damit** die Sicherheit des Hubs nicht an unserem Team hängt, sondern an einem System, das HLG selbst betreibt.

DAS LIEFERT IHR AB

- **Lernprodukt 17 (Track A):** eine unterschriftsreife Leitlinie, ein Rollenmodell, einen Abgleich eurer Maßnahmen mit Grundschutz-Bausteinen und Anhang A, den Umsetzungsgrad mit Rechenweg und einen ISMS-Fahrplan über zwölf Monate mit Kennzahlen und Kosten
- **Lernprodukt 18 (Track B):** ein Sicherheitskonzept mit allen Lernprodukten aus Teil 1 bis 6, einen Rückblick seit M1, eine vorbereitete Antwort zu NIS 2 und den Meldefristen und ein geführtes Übergabegespräch (Meilenstein M4)
- Wissensspeicher-Blatt mit drei Prüffragen

AKZEPTANZBEDINGUNGEN

Vom Kunden. Die Karte ist erst fertig, wenn alle Punkte im Review abgenommen sind. Ein Zurück ohne Begründung zählt nicht.

- ☐ AB 1 · Die Leitlinie passt auf eine Seite, nennt Geltungsbereich, Sicherheitsziele, Verantwortung der Geschäftsleitung und Verpflichtung zur Verbesserung und ist so formuliert, dass die Geschäftsleitung sie unterschreiben kann.
- ☐ AB 2 · Das Rollenmodell nennt für jede Rolle Aufgabe, Befugnis und Stelle; die Informationssicherheitsbeauftragte berichtet direkt an die Geschäftsleitung.
- ☐ AB 3 · Jedes Lernprodukt aus Teil 1 bis 5 ist einer Phase des ISMS-Zyklus zugeordnet; die Lücken sind benannt.
- ☐ AB 4 · Der Abgleich ordnet jede eurer Maßnahmen mindestens einem Grundschutz-Baustein und einer Maßnahme aus Anhang A zu.
- ☐ AB 5 · Der Umsetzungsgrad ist gewichtet gerechnet, der Rechenweg ist für Dritte nachvollziehbar.
- ☐ AB 6 · Der ISMS-Fahrplan deckt zwölf Monate ab, nennt Verantwortliche, Kosten und fünf Kennzahlen mit Zielwerten.
- ☐ AB 7 · Das Sicherheitskonzept führt alle Lernprodukte nach einer erkennbaren Gliederung zusammen und enthält einen Rückblick: was seit M1 geändert wurde und weshalb.
- ☐ AB 8 · Die Antwort zu NIS 2 enthält Sektor, Größe, Ergebnis, Unsicherheiten und eine Empfehlung; die Meldefristen sind an einem Beispiel mit Uhrzeit bestimmt.

Unsere eigene AB, mit dem Auftraggeber vereinbart (AB 9):

_____

KREUZREVIEW | GESCHÄFTSLEITUNG HLG · M4 ÜBERGABEGESPRÄCH | DATUM

DAS STEUERT IHR · STUFE 4

Dazu formuliert ihr eine AB selbst und vereinbart sie mit dem Auftraggeber (Lehrkraft). Der Kurs gibt nur die Story vor.

UNSER SPRINTZIEL, IN EIGENEN WORTEN

_____

_____

Die Lage ändert sich · Lernangebot 17. Die Geschäftsleitung halbiert das Budget. Es gibt keine eigene ISB, nur das Werkzeug, die Schulung und die Hälfte der externen Begleitung. Nach eurer Einschätzung sinkt die Wahrscheinlichkeit eines Erpressungsangriffs dann nur auf 8 % je Jahr, und der Stillstand dauert 24 Stunden, weil niemand die Abläufe übt. Prüft euren Fahrplan: Was fällt weg, was ist das erste Jahr jetzt noch wert, und was sagt ihr der Geschäftsleitung?

Die Lage ändert sich · Lernangebot 18. Zwei Wochen nach der Übergabe meldet sich die IT-Leitung: Der Pharmakunde verlangt bis Jahresende einen Nachweis nach ISO/IEC 27001, sonst wechselt er den Spediteur. Die Geschäftsleitung fragt, ob das in eurem Fahrplan zu schaffen ist. Was ändert sich am Fahrplan, was ist realistisch, und was schlagt ihr vor?

STORYCARD · TEIL 6 · RÜCKSEITE

ANSCHLUSS

DAS BRINGT IHR MIT

- eure Lernprodukte aus Teil 1 bis 5 (Wissensspeicher-Blätter und Dokumentation)
- die Fachgrundlage dieses Teils, vor allem den Abschnitt zu ISO/IEC 27001 und IT-Grundschutz
- Zugang zum IT-Grundschutz-Kompendium und zu den BSI-Standards 200-1 und 200-2 auf der Seite des BSI
- einen Rechner je Zweiergruppe für Tabellen und Konzept; ein Labor braucht ihr in Teil 6 nicht

HIER GEHT ES WEITER

- Wahlphase: Wahlstories mit CreditPoints, darunter die Meta-Story mit eurer eigenen Story
- Kontrolle Teil 6 und dein Kompetenzmodell im Kurs
- Eure Retrospektive auf dieser Rückseite, der nächste Sprint kommt vom Board

KOMPETENZMODELL

Kompetenz aus dem Lehrplan · führen ein Informationssicherheitsmanagementsystem ein und übergeben ein Sicherheitskonzept. **Gehört:** du weißt, dass es das gibt. **Verstanden:** du wendest es mit Unterlagen an. **Erklärt:** du bringst es anderen ohne Unterlagen bei. Kreuze im Planning und in der Retrospektive an, mit zwei Farben.

ICH KANN …	GEHÖRT	VERSTANDEN	ERKLÄRT
… erklären, was ein ISMS ist und wie es sich von einzelnen Sicherheitsmaßnahmen unterscheidet.	☐	☐	☐
… den Zyklus Planen, Umsetzen, Prüfen, Verbessern auf die Informationssicherheit eines Betriebs anwenden.	☐	☐	☐
… eine Leitlinie zur Informationssicherheit entwerfen und Rollen wie die Informationssicherheitsbeauftragte festlegen.	☐	☐	☐
… das Vorgehen nach BSI-Standard 200-1 und 200-2 und den Aufbau des IT-Grundschutz-Kompendiums beschreiben.	☐	☐	☐
… ISO/IEC 27001 mit Anhang A und IT-Grundschutz vergleichen und Maßnahmen beiden zuordnen.	☐	☐	☐
… den Umsetzungsgrad von Anforderungen gewichtet berechnen und Kennzahlen für ein ISMS festlegen.	☐	☐	☐
… prüfen, ob ein Unternehmen unter NIS 2 fällt, und die Meldefristen bei einem Sicherheitsvorfall bestimmen.	☐	☐	☐
… die Kosten eines ISMS gegen den erwarteten vermiedenen Schaden abwägen.	☐	☐	☐
… ein Sicherheitskonzept in einem Fachgespräch mit der Geschäftsleitung übergeben und Rückfragen beantworten.	☐	☐	☐
… rückblickend begründen, was ich seit dem ersten Meilenstein anders entschieden habe und weshalb.	☐	☐	☐

Was bringt mich jetzt am meisten weiter? _____

RETROSPEKTIVE

DAS HAT GETRAGEN

DAS HAT GEBREMST

DAS ÄNDERN WIR IM NÄCHSTEN SPRINT

WO STEHT DIE KARTE?

☐ OFFEN ☐ IN ARBEIT ☐ REVIEW ☐ FERTIG