STORYCARD · TEIL 2 · SCHUTZBEDARF UND RISIKO · SPRINT 2 · TRACK A UND B

Was kostet eine Stunde ohne Frachtannahme?

Der Datenschutz ist geklärt, das Datenflussbild aus Teil 1 liegt auf dem Tisch. Jetzt fragt die Geschäftsleitung von HLG das, was sie seit dem Angriff in der Nachbarhalle umtreibt: Was müssen wir schützen, wie schlimm wäre es, und was kostet uns das? Euer Sicherheitsteam beantwortet es nach der Methode des IT-Grundschutzes und in Euro.

Sprint 2 | **30 Stunden** | **20 CP** | **Lernangebot 4 und 5 und 6** | **Meilenstein M1**

Als Sicherheitsteam von Querwind **wollen wir** mit der Geschäftsleitung von HLG festlegen, welche Anwendungen, Systeme und Räume des Hubs welchen Schutz brauchen, welche Gefährdungen ihnen drohen und welche Maßnahmen sich rechnen, **damit** HLG nicht nach Gefühl investiert, sondern nach einer Rechnung, die es nachvollziehen und unterschreiben kann.

DAS LIEFERT IHR AB

- **Lernprodukt 4 (Track A):** eine Strukturanalyse mit allen Prozessen, Anwendungen, Systemen, Räumen und Netzen des Hubs und eine Schutzbedarfsfeststellung mit Begründung je Anwendung und Vererbung bis zum Netz
- **Lernprodukt 5 (Track A):** eine Gefährdungsübersicht mit Nummern nach BSI-Standard 200-3, eine Risikomatrix für die drei Zielobjekte, den erwarteten jährlichen Schaden je Gefährdung und die Verfügbarkeit des Frachtsystems heute
- **Lernprodukt 6 (Track B):** einen Maßnahmenplan mit Kosten, Wirkung, Wirtschaftlichkeit, Reihenfolge und Zuständigkeit, eine Risikomatrix nach den Maßnahmen, das ausgewiesene Restrisiko und eine Entscheidungsvorlage für die Geschäftsleitung
- 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 Strukturanalyse nennt alle Geschäftsprozesse, Anwendungen, virtuellen Maschinen, Hosts, Räume und Netze des Hubs und zeigt, was worauf läuft.
- ☐ AB 2 · Die Schutzbedarfskategorien sind mit Grenzen in Euro und Stunden festgelegt und von der Geschäftsleitung bestätigt.
- ☐ AB 3 · Jede Anwendung hat einen Schutzbedarf für Vertraulichkeit, Integrität und Verfügbarkeit mit einer Begründung aus einem Schadensszenario.
- ☐ AB 4 · Server, Serverraum und Netz haben einen vererbten Schutzbedarf; Maximumprinzip, Kumulations- und Verteilungseffekt sind dort, wo sie greifen, benannt.
- ☐ AB 5 · Die Gefährdungsanalyse für Frachtsystem, Kühlüberwachung und Zufahrt nennt elementare Gefährdungen mit Nummer und ist in einer Risikomatrix eingestuft.
- ☐ AB 6 · Ausfallkosten, erwarteter jährlicher Schaden vor und nach den Maßnahmen und die Wirtschaftlichkeit jeder Maßnahme sind mit Rechenweg nachvollziehbar.
- ☐ AB 7 · Die Entscheidungsvorlage nennt Empfehlung, Kosten, Restrisiko und die Unterschrift, mit der die Geschäftsleitung das Restrisiko trägt.

Unsere eigenen Kriterien, im Planning mit dem Auftraggeber vereinbart:

_____

KREUZREVIEW | GESCHÄFTSLEITUNG HLG · M1 | DATUM

DAS STEUERT IHR · STUFE 2

Dazu formuliert ihr ein eigenes Kriterium, prüft es im Review und bewertet es in der Retrospektive. Der mögliche Weg ist nur noch eingeklappt.

UNSER SPRINTZIEL, IN EIGENEN WORTEN

_____

_____

Die Lage ändert sich · Lernangebot 4. HLG übernimmt einen zweiten Pharmakunden. Er verlangt, dass seine Temperaturdaten nicht nur vollständig, sondern auch nachweisbar unverändert sind, und er will sie selbst über die Sendungsverfolgung im Web einsehen. Was ändert sich an eurem Schutzbedarf für Kühlüberwachung, Sendungsverfolgung und DMZ, und für welches Schutzziel?

STORYCARD · TEIL 2 · RÜCKSEITE

ANSCHLUSS

DAS BRINGT IHR MIT

- euer Datenflussbild aus Teil 1 und die Liste der personenbezogenen Daten
- die Fachgrundlage dieses Teils, vor allem die Tabellen zu Schutzbedarf und Risikomatrix
- die gegebenen Werte unten; für die Bausteine das IT-Grundschutz-Kompendium Edition 2023 im Netz des BSI
- eine Tabellenkalkulation je Team; ein Labor braucht ihr in Teil 2 nicht

HIER GEHT ES WEITER

- Sprint 3: Teil 3 · Datensicherung, mit eurem Schutzbedarf für die Verfügbarkeit
- Kontrolle Teil 2 und dein Kompetenzmodell im Kurs
- Eure Retrospektive auf dieser Rückseite, der nächste Sprint kommt vom Board

KOMPETENZMODELL

Kompetenz aus dem Lehrplan · berücksichtigen alle Aspekte der Datensicherung und -verfügbarkeit. **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
… aus einem Datenflussbild die Geschäftsprozesse, Anwendungen, IT-Systeme, Räume und Netze eines Betriebs herauslesen (Strukturanalyse).	☐	☐	☐
… den Schutzbedarf einer Anwendung für Vertraulichkeit, Integrität und Verfügbarkeit mit Schadensszenarien begründen.	☐	☐	☐
… den Schutzbedarf nach Maximumprinzip, Kumulationseffekt und Verteilungseffekt auf Server, Räume und Netze übertragen.	☐	☐	☐
… die betriebliche Abhängigkeit von Daten an einem Geschäftsprozess zeigen und in Euro beziffern.	☐	☐	☐
… eine Gefährdungsanalyse mit den elementaren Gefährdungen des BSI erstellen.	☐	☐	☐
… Risiken nach Häufigkeit und Auswirkung einstufen und in einer Risikomatrix darstellen.	☐	☐	☐
… eine Risikomaßnahmenplanung mit Kosten, Wirkung und Restrisiko erstellen und die Umsetzung planen.	☐	☐	☐
… Verfügbarkeit in Prozent und die erlaubte Ausfallzeit im Jahr ineinander umrechnen.	☐	☐	☐
… der Geschäftsleitung eine Entscheidung so vorlegen, dass sie sie ohne Fachwissen treffen und unterschreiben kann.	☐	☐	☐
… erkennen, wo meine Bewertung auf Schätzungen beruht, und das offen ausweisen.	☐	☐	☐

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