STORYCARD · TEIL 5 · TECHNISCHE SCHUTZMASSNAHMEN · SPRINT 5 · TRACK A UND B

Wem vertraut der Handscanner?

Die Risiken sind bewertet, der Labortest aus Teil 4 hat gezeigt, wo es offen ist. Jetzt setzt euer Sicherheitsteam die technischen Schutzmaßnahmen um: Vertrauen über Zertifikate, sichere Fernzugriffe, verschlüsselte Datenspeicher, Zugangsschutz, Angriffserkennung und ein Alarmierungskonzept für die Nacht.

Sprint 5 | **30 Stunden** | **20 CP** | **Lernangebot 13 und 14 und 15 und 16** | **Meilenstein M3**

Als Sicherheitsteam von Querwind **wollen wir** festlegen und im Labor zeigen, wem jedes Gerät im Hub vertraut, wie Fernzugriffe gesichert sind, was verschlüsselt wird, wer sich wie anmeldet und wie ein Angriff in der Nacht bemerkt und gemeldet wird, **damit** die Geschäftsleitung bei Meilenstein M3 sieht: Die Maßnahmen aus Teil 2 stehen nicht nur auf Papier.

DAS LIEFERT IHR AB

- **Lernprodukt 13 (Track A):** einen PKI-Plan für drei Standorte mit Hierarchie, Laufzeiten, Namensschema, Mengengerüst der Zertifikate und einem Sperrprozess mit Verantwortlichen
- **Lernprodukt 14 (Track A):** einen SSH-Zugang mit Schlüsseln im Labor mit Protokoll, TLS-Vorgaben für Frachtsystem und Sendungsverfolgung und einen Plan für die Fernwartung
- **Lernprodukt 15 (Track B):** ein Verschlüsselungskonzept für Datenträger mit Wiederherstellung, ein Virenschutzkonzept für alle Geräteklassen, eine Passwort- und MFA-Regel und einen Schutz der Anmeldung an der Sendungsverfolgung
- **Lernprodukt 16 (Track B):** ein IDS im Labor mit eigener Regel für den Portscan, gemessene Erkennungs- und Fehlalarmrate mit Bewertung und ein Alarmierungskonzept für die Nachtschicht
- 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 · Der PKI-Plan nennt Stamm- und ausstellende Zertifizierungsstellen, Laufzeiten, Namensschema, die Zahl der Zertifikate und der Erneuerungen im Jahr mit Rechenweg und einen Sperrprozess mit Verantwortlichen.
- [ ] AB 2 · Im Labor ist ein SSH-Zugang mit Schlüsseln eingerichtet, die Anmeldung mit Passwort ist abgeschaltet; das Protokoll zeigt beides.
- [ ] AB 3 · Für die Sendungsverfolgung ist festgelegt, welches Zertifikat, welche TLS-Versionen und wer die Erneuerung überwacht.
- [ ] AB 4 · Für jeden Datenträger der Laptops, Handscanner und Server steht, ob und wie er verschlüsselt wird und wo der Wiederherstellungsschlüssel liegt.
- [ ] AB 5 · Virenschutzkonzept, Passwort- und MFA-Regel und Schutz der Anmeldung an der Sendungsverfolgung sind begründet und für die Schichtleitung verständlich formuliert.
- [ ] AB 6 · Der Sensor im Labor meldet den Portscan aus Teil 4; Erkennungs- und Fehlalarmrate sind gemessen und bewertet.
- [ ] AB 7 · Das Alarmierungskonzept legt Melde- und Eskalationswege, Zeiten und Bereitschaft für die Nachtschicht fest.
- [ ] AB 8 · Der Fernwartungszugang des Herstellers ist entworfen, im Labor geprüft und erreicht nachweislich nur die Röntgenarbeitsplätze.

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

_____

KREUZREVIEW _____ IT-LEITUNG HLG · M3 _____ 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 13. Das Stationsbüro an einem zweiten Flughafen soll mit einem Partner in Übersee Sendungsdaten austauschen. Der Partner hat eine eigene PKI und schlägt vor, dass ihr sein Stammzertifikat in alle Geräte von HLG aufnehmt. Was würde das bedeuten, und welche Lösung würdet ihr stattdessen vorschlagen?

STORYCARD · TEIL 5 · RÜCKSEITE

ANSCHLUSS

DAS BRINGT IHR MIT

- eure Ergebnisse aus Teil 2 (Maßnahmenplan) und Teil 4 (Laborbefunde)
- das Labornetz mit Angreifer-System, Zielsystem und Server je Team; den Raspberry Pi als Sensor
- die Fachgrundlage dieses Teils, vor allem die Tabellen zu Schlüssellängen und Zertifikaten
- die schriftliche Freigabe für Angriffe im Labor aus dem Projektauftrag (§202a bis §202c StGB)

HIER GEHT ES WEITER

- Sprint 6: Teil 6 · ISMS, eure Maßnahmen gehen ins Sicherheitskonzept
- Kontrolle Teil 5 und dein Kompetenzmodell im Kurs
- Eure Retrospektive auf dieser Rückseite, der nächste Sprint kommt vom Board

KOMPETENZMODELL

Kompetenz aus dem Lehrplan · planen aktive und passive Schutzmaßnahmen. **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
… aktive und passive Schutzmaßnahmen für ein Unternehmensnetz planen und gegeneinander abwägen.	☐	☐	☐
… symmetrische und asymmetrische Verschlüsselung, Hashfunktion und digitale Signatur unterscheiden.	☐	☐	☐
… eine Schlüsselverwaltung in Unternehmens-Netzwerken (PKI) mit Stamm- und ausstellender Zertifizierungsstelle planen.	☐	☐	☐
… Zertifikate lesen, ihre Kette prüfen und einen Sperrprozess (CRL, OCSP) beschreiben.	☐	☐	☐
… einen sicheren Fernzugriff (remote login mit secure shell (SSH)) mit Schlüsseln einrichten.	☐	☐	☐
… TLS, die Nachfolge der SSL-(Secure Socket Layer) Techniken, für einen Webdienst richtig nutzen.	☐	☐	☐
… Datenspeicher-Verschlüsselung, Virenschutz und Zugangssicherung z. B. mit Captcha und Passwortschutz begründet auswählen.	☐	☐	☐
… ein Intrusion-Detection System einrichten und ein Alarmierungskonzept entwerfen.	☐	☐	☐
… Fehlalarme gegen übersehene Angriffe abwägen und die Entscheidung vertreten.	☐	☐	☐
… mit der IT-Leitung und einem Dienstleister von außen Regeln für Zugänge aushandeln.	☐	☐	☐

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