STORYCARD · TEIL 5 · KRYPTOGRAFIE UND ZERTIFIKATE · SPRINT 4 · TRACK A

Wem können die Kunden trauen?

Die Sendungsverfolgung ist von außen erreichbar, und genau das macht sie angreifbar. In Teil 5 sorgt ihr dafür, dass Kunden der Seite trauen können, dass niemand unterwegs mitliest und dass sich Mitarbeitende so anmelden, dass ein gestohlenes Passwort allein nicht reicht.

Sprint 4 · Track A | **20 Stunden** | **10 CP** | **Lernangebot 10 und 11** | **Vorarbeit für M4**

Als IT-Leitung HLG **will ich** ein Schlüssel- und Zertifikatskonzept, **damit** Kunden und Standorte der Verbindung trauen können.

DAS LIEFERT IHR AB

- **Lernprodukt 10:** eine Übersicht, welches Verfahren welches Schutzziel sichert, einen von Hand nachgerechneten Schlüsseltausch mit der Sicht des Mithörers und eine Empfehlung für Schlüssellängen mit Quelle
- **Lernprodukt 11:** ein Zertifikat für track.hlg.example aus dem Labor, eine geprüfte Zertifikatskette, einen Plan für Ablauf und Erneuerung und ein Anmeldekonzept für Mitarbeitende und Kunden, zusammen das Schlüssel- und Zertifikatskonzept
- 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 Übersicht ordnet jedem Verfahren (symmetrisch, asymmetrisch, hybrid, Hashwert, Signatur, Zertifikat, Schlüsseltausch) die Schutzziele zu, jede Zuordnung mit einem Grund.
- ☐ AB 2 · Der Schlüsseltausch mit p = 23, g = 5 und den geheimen Zahlen 6 und 15 ist von Hand nachgerechnet, beide Seiten kommen auf denselben Schlüssel, und es ist aufgeschrieben, was der Mithörer sieht.
- ☐ AB 3 · Für jeden Einsatz (Webverbindung, Signatur, VPN) ist eine Schlüssellänge festgelegt, mit Quelle und Stand der Empfehlung.
- ☐ AB 4 · Die Zertifikatskette für track.hlg.example ist Stufe für Stufe geprüft (Name, Aussteller, Gültigkeit, Berechtigung), der Fehler in der Prüftabelle ist gefunden und begründet.
- ☐ AB 5 · Ablauf und Erneuerung sind geregelt: Laufzeit, Beginn der Erneuerung, Warnungen, zuständige Person mit Vertretung, auch für das Wochenende.
- ☐ AB 6 · Die Anmeldung ist entworfen: Mitarbeitende mit zweitem Faktor, Kunden ohne Konto mit Sendungsnummer und Postleitzahl, Rateaufwand berechnet und Abfragegrenze festgelegt.
- ☐ AB 7 · Das Wissensspeicher-Blatt ist vollständig, die Kontrolle Teil 5 ist bearbeitet.

Unsere eigene AB, mit der IT-Leitung vereinbart (AB 8):

_____

KREUZREVIEW | IT-LEITUNG HLG · M4 MIT TEIL 6 | DATUM

DAS STEUERT IHR · STUFE 4

Dazu formuliert ihr eine AB selbst und vereinbart sie mit der IT-Leitung. Der Kurs gibt nur die Story vor.

UNSER SPRINTZIEL, IN EIGENEN WORTEN

_____

_____

Die Lage ändert sich · Lernangebot 10. Für das alte Scannerfunkgerät im Straßenlager bietet der Hersteller nur ein Verfahren mit 64-Bit-Schlüsseln an. Ein Kollege meint, das sei „für Scannerdaten genug“. Berechne, wie lange das Durchprobieren mit den Werten dieses Lernangebots dauert, beurteile das Risiko für HLG und schlag eine Lösung vor.

Die Lage ändert sich · Lernangebot 11. Das Zertifikat der Sendungsverfolgung läuft am Samstag, 29.05.2027, ab. Die automatische Erneuerung ist seit einer Änderung an der Firewall still gescheitert, und am Wochenende hat niemand Bereitschaft. Überprüfe deinen Plan aus Aufgabe 11.4: Beschreibe, was die Kunden am Samstagmorgen um 5:30 Uhr sehen, finde die Lücke in deinem Plan und ergänze ihn so, dass der Fall nicht eintritt.

STORYCARD · TEIL 5 · RÜCKSEITE

ANSCHLUSS

DAS BRINGT IHR MIT

- euer Dienstekonzept und die DMZ aus Teil 3 und Teil 4 (Verteiler, web1, web2)
- Taschenrechner oder Tabellenkalkulation für die Rechnungen mit Rest
- eine virtuelle Maschine mit Linux für den Laborvorschlag in Lernangebot 11
- Zugang zu einer aktuellen Empfehlung für Schlüssellängen (Lernangebot 10, Aufgabe 10.6)

HIER GEHT ES WEITER

- Teil 6 läuft parallel; euer Konzept sichert den Tunnel, zusammen ergeben beide M4
- Kontrolle Teil 5 und dein Kompetenzmodell im Kurs
- Eure Retrospektive auf dieser Rückseite, der nächste Sprint kommt vom Board

KOMPETENZMODELL

Kompetenz aus dem Lehrplan · ermöglichen sichere Kommunikation über unsichere Verbindungswege. **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
… die drei Schutzziele Vertraulichkeit, Integrität und Authentizität an einem Beispiel aus der Sendungsverfolgung unterscheiden.	☐	☐	☐
… symmetrische, asymmetrische und hybride Verschlüsselung vergleichen und begründen, weshalb eine Webverbindung hybrid arbeitet.	☐	☐	☐
… erklären, wie Hashwert und Signatur zusammen Integrität und Authentizität sichern.	☐	☐	☐
… einen Schlüsseltausch nach Diffie-Hellman mit kleinen Zahlen von Hand nachrechnen und sagen, was ein Mithörer sieht.	☐	☐	☐
… die Sicherheit von Schlüssellängen über den Rechenaufwand abschätzen und eine aktuelle Empfehlung mit Quelle nennen.	☐	☐	☐
… eine Zertifikatskette Stufe für Stufe prüfen und einen Fehler darin finden.	☐	☐	☐
… ein Zertifikat mit Schlüssel, Antrag und eigener Test-Zertifizierungsstelle auf einer virtuellen Maschine erstellen.	☐	☐	☐
… ein Anmeldekonzept für Mitarbeitende mit zweitem Faktor und für Kunden ohne Konto entwerfen und den Rateaufwand berechnen.	☐	☐	☐
… der IT-Leitung HLG ohne Fachsprache erklären, weshalb ein abgelaufenes Zertifikat die Kunden aussperrt.	☐	☐	☐
… im Team Zuständigkeiten für Ablauf und Erneuerung so festlegen, dass sie auch am Wochenende tragen.	☐	☐	☐
… meine Unsicherheiten bei Formeln mit Potenz und Rest erkennen und gezielt an kleinen Zahlen üben.	☐	☐	☐

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