STORYCARD · TEIL 4 · BEDROHUNGEN UND ANGRIFFE · SPRINT 4 · TRACK A UND B

Wie käme ein Angreifer in die Halle?

Schutzbedarf, Risiken und Sicherung sind geplant. Jetzt schaut euer Sicherheitsteam mit den Augen eines Angreifers auf den Hub: Was wird gerade angegriffen, wie gehen Täter vor, und wo käme jemand heute in die Halle? Ihr lest Warnungen, baut einen Angriffsbaum und testet im eigenen Labornetz.

Sprint 4 | **30 Stunden** | **15 CP** | **Lernangebot 10 und 11 und 12** | **Meilenstein M2**

Als Sicherheitsteam von Querwind **wollen wir** ein Lagebild aus aktuellen Warnungen erstellen, einen Angriffsbaum für den Hub mit Abwehr je Angriffsart bauen und im isolierten Labornetz zeigen, wie ein Test abläuft und was er findet, **damit** die Geschäftsleitung bei Meilenstein M2 weiß, welche Tore offen sind und welche Maßnahmen aus Teil 2 zuerst kommen.

DAS LIEFERT IHR AB

- **Lernprodukt 10 (Track A):** ein Lagebild auf einer Seite: Quellen mit Datum, jede Warnung mit CVSS-Einstufung und eigener Dringlichkeit für den Hub, Maßnahmen mit Frist und Verantwortlichen
- **Lernprodukt 11 (Track A):** einen Angriffsbaum für den Hub mit dem Ziel „Frachtannahme steht“ an der Spitze, mindestens sechs Angriffsarten aus dem Lehrplan, je Ast einer Abwehr mit Schutzziel und den Rechnungen zu Passwortraum und Ausfallkosten
- **Lernprodukt 12 (Track B):** eine unterschriebene Freigabe und einen Testbericht mit Zusammenfassung für die Leitung, Liste der Dienste mit Versionen, Abgleich mit Schwachstellendatenbanken, Bewertung, Abwehrvorschlägen und Nachtest
- 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 · Das Lagebild passt auf eine Seite, nennt die Quellen mit Datum, stuft jede Warnung mit CVSS und mit dem Bezug auf den Hub ein und sagt, was bis wann zu tun ist.
- ☐ AB 2 · Der Angriffsbaum hat das Ziel „Frachtannahme steht“ an der Spitze, enthält mindestens sechs der Angriffsarten aus dem Lehrplan und nennt je Ast eine Abwehr mit Schutzziel.
- ☐ AB 3 · Die Rechnungen zum Passwortraum und zu den Ausfallkosten eines Überlastangriffs sind mit Formel, Einheiten und Annahmen nachvollziehbar.
- ☐ AB 4 · Vor dem Labortest lag eine schriftliche Freigabe mit Ziel, Umfang, Zeitraum, Methoden und Abbruchkriterien vor; der Test lief nur im isolierten Labornetz gegen das eigene Zielsystem.
- ☐ AB 5 · Der Testbericht nennt jeden gefundenen Dienst mit Version, den Abgleich mit einer Schwachstellendatenbank, eine Bewertung und je Befund einen Abwehrvorschlag.
- ☐ AB 6 · Der offene Fall der Handscanner ist entschieden: Lage, Sofortmaßnahmen, spätere Maßnahmen und Zuständigkeiten sind begründet.

Unsere eigenen Kriterien, im Planning mit dem Auftraggeber vereinbart:

_____

KREUZREVIEW _____ GESCHÄFTSLEITUNG HLG · M2 _____ DATUM _____

DAS STEUERT IHR · STUFE 3

Dazu entscheidet ihr, welche Inputs ihr euch holt, und schreibt eure Schritte selbst. Der Kurs gibt Story und den Kern der AB vor.

UNSER SPRINTZIEL, IN EIGENEN WORTEN

_____

_____

Die Lage ändert sich · Lernangebot 10. Zwei Tage nach eurem Lagebild ergänzt der Hersteller des Webframeworks seine Meldung UE-2026-013: Die Lücke wird jetzt in Angriffen auf Paketdienste aktiv ausgenutzt, über präparierte Links in Mails an Kunden. Der Basiswert bleibt 6,1. Was ändert sich in eurem Lagebild, und weshalb ändert sich der Basiswert nicht?

STORYCARD · TEIL 4 · RÜCKSEITE

ANSCHLUSS

DAS BRINGT IHR MIT

- eure Ergebnisse aus Teil 2 (Strukturanalyse, Risikomatrix, Maßnahmenplan)
- das Labornetz eures Teams: Angreifer-System, absichtlich verwundbares Zielsystem, Server, ohne Verbindung nach außen
- die schriftliche Freigabe aus Lernangebot 12, unterschrieben von eurer Lehrkraft (§202a bis §202c StGB)
- Zugang zu öffentlichen Quellen: Warnungen von CERT-Bund, CVE-Liste, Hinweise der Hersteller

HIER GEHT ES WEITER

- Sprint 5: Teil 5 · Technische Schutzmaßnahmen gegen eure Befunde aus dem Labor
- Kontrolle Teil 4 und dein Kompetenzmodell im Kurs
- Eure Retrospektive auf dieser Rückseite, der nächste Sprint kommt vom Board

KOMPETENZMODELL

Kompetenz aus dem Lehrplan · halten sich aktuell über Entwicklungen der Bedrohungen und Angriffsszenarien. **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
… mich aktuell über Entwicklungen der Bedrohungen und Angriffsszenarien halten und wissen, wo ich nachsehe.	☐	☐	☐
… die Schutzziele Authentizität, Vertraulichkeit, Verbindlichkeit, Integrität und Verfügbarkeit an Beispielen erklären.	☐	☐	☐
… Angriffsszenarien und Tools wie Portscan, Phishing, Visual Hacking, Keylogger, Cross-Site-Scripting, Man-in-the-middle, DoS, Botnetze und Ransomware erklären.	☐	☐	☐
… passive und aktive Angriffe unterscheiden und je eine Abwehr nennen.	☐	☐	☐
… aktuelle Vulnerabilitäten aus CERT-Meldungen, Schwachstellendatenbanken und Security-Boards recherchieren und mit CVSS einordnen.	☐	☐	☐
… einen Penetrationstest im isolierten Labornetz mit schriftlicher Freigabe planen, durchführen und berichten.	☐	☐	☐
… die Vorgehensweisen der Cyber-Kriminalität als Angriffskette beschreiben.	☐	☐	☐
… aus vielen Warnungen die wenigen herausfiltern, die für den Betrieb dringend sind.	☐	☐	☐
… einer Geschäftsleitung eine Sicherheitslage auf einer Seite verständlich machen.	☐	☐	☐
… erkennen, wo ich rechtlich und fachlich an eine Grenze komme, und dort stoppen.	☐	☐	☐

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