STORYCARD · TEIL 4 · FIREWALL UND DMZ · SPRINT 4

Wer darf von außen bis wohin?

Die Sendungsverfolgung ist seit Meilenstein M2 von außen erreichbar. Damit ist das Hub auch für alle anderen erreichbar. Die IT-Leitung HLG will jetzt wissen, wer von außen bis wohin darf, und für jede offene Tür einen Grund hören.

Sprint 4 | **30 Stunden** | **15 CP** | **Lernangebot 8 und 9** | **M3 · Abgesichert**

Als IT-Leitung HLG **will ich**, dass von außen nur erreichbar ist, was erreichbar sein muss, **damit** ein Angriff auf die Sendungsverfolgung nicht im Hallennetz endet.

DAS LIEFERT IHR AB

- **Lernprodukt 8:** eine Gegenüberstellung der drei Firewall-Varianten mit je einem Angriff, den sie abwehren, und einem, den sie nicht abwehren, und eine begründete Empfehlung, welche Varianten HLG an welcher Stelle braucht
- **Lernprodukt 9:** ein Zonenmodell mit DMZ 172.16.10.0/24, eine vollständige Filtertabelle, eingerichtete Filter mit Nachweis, ein Testprotokoll, die Angriffsszenarien je Zone und eine begründete Entscheidung für eine oder zwei Stufen
- 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 Zonenmodell ordnet jedes System des Hubs genau einer Zone zu, die DMZ 172.16.10.0/24 ist eingezeichnet, die Architektur (eine oder zwei Stufen) ist begründet.
- ☐ AB 2 · Die Filtertabelle hat für jede Regel Nr., Quelle, Ziel, Dienst/Port, Richtung, Aktion und Grund; keine Regel erlaubt „beliebig“ dort, wo eine engere Angabe möglich ist.
- ☐ AB 3 · Die letzte Regel verweigert alles Übrige und protokolliert es.
- ☐ AB 4 · Aus der DMZ ins interne Netz führt höchstens eine eng begründete Ausnahme; die Verwaltung der Firewall ist von außen nicht erreichbar.
- ☐ AB 5 · Die Filter sind im Labor über eine Oberfläche und als Konfigurationsdatei eingerichtet, mit Nachweis.
- ☐ AB 6 · Das Testprotokoll zeigt mindestens zehn Testverbindungen mit erwartetem und beobachtetem Ergebnis, darunter mindestens vier, die verweigert werden müssen.
- ☐ AB 7 · Für jede Zone ist mindestens ein Angriffsszenario mit Folge für HLG und Gegenmaßnahme beschrieben, gestützt auf die Gegenüberstellung der drei Firewall-Varianten (je ein Angriff, den sie abwehren, und einer, den sie nicht abwehren).

Unsere eigenen Kriterien, im Planning mit dem Auftraggeber vereinbart:

_____

IT-LEITUNG HLG | IT-LEITUNG HLG · M3 | 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 8. HLG will, dass sich Großkunden an der Sendungsverfolgung anmelden und eigene Sendungen anlegen können. Prüfe deine Gegenüberstellung: Welcher Angriff wird dadurch wichtiger, und reicht deine Empfehlung aus 8.6 noch?

Die Lage ändert sich · Lernangebot 9. Der Hersteller der Röntgenanlage in der Frachtkontrolle will einen dauerhaften Zugang von außen auf den Steuerrechner 10.10.20.200, „damit wir bei Störungen sofort helfen können“. Prüfe dein Zonenmodell und deine Filtertabelle: Was müsstest du dafür ändern, und was schlägst du der IT-Leitung stattdessen vor?

STORYCARD · TEIL 4 · RÜCKSEITE

ANSCHLUSS

DAS BRINGT IHR MIT

- euer Adress- und Dienstekonzept aus Teil 2 und Teil 3 (M2)
- den Zonenplan und die gegebenen Werte aus Lernangebot 9
- im Labor eine Firewall in einer virtuellen Maschine mit drei Schnittstellen (Laborvorschlag: OPNsense) und je einen Testrechner außen, in der DMZ und innen, alternativ Packet Tracer
- Wireshark für den Blick auf verweigerte Pakete

HIER GEHT ES WEITER

- Sprint 5: Teil 5 · Kryptografie und Zertifikate, danach in Sprint 6 Teil 6 · VPN
- Kontrolle Teil 4 und dein Kompetenzmodell im Kurs
- Eure Retrospektive auf dieser Rückseite, der nächste Sprint kommt vom Board

KOMPETENZMODELL

Kompetenz aus dem Lehrplan · wählen geeignete Methoden zur Zugangskontrolle sowie zum Schutz vor Angriffen aus und nutzen diese. **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
… Paketfilter, zustandsbehaftete Filter und Filter auf Anwendungsebene nach ihrer Prüftiefe unterscheiden.	☐	☐	☐
… typische Angriffe (Portscan, Spoofing, Überlastung, Ausnutzen eines Webdienstes, Phishing) erklären und der Schicht zuordnen, auf der sie wirken.	☐	☐	☐
… für jede Firewall-Variante einen Angriff nennen, den sie abwehrt, und einen, den sie nicht abwehrt.	☐	☐	☐
… ein Netz in Sicherheitszonen mit DMZ aufteilen und eine ein- oder zweistufige Anordnung begründen.	☐	☐	☐
… eine vollständige Filtertabelle mit Quelle, Ziel, Dienst, Richtung, Aktion und Grund entwerfen.	☐	☐	☐
… Filterregeln über eine Oberfläche und als Konfigurationsdatei einrichten.	☐	☐	☐
… ein Regelwerk mit geplanten Testverbindungen prüfen und das Ergebnis protokollieren.	☐	☐	☐
… Angriffsszenarien je Zone beschreiben und ihre Folgen für HLG abschätzen.	☐	☐	☐
… jede Regel gegenüber der IT-Leitung so begründen, dass sie ohne Fachwissen nachvollziehbar ist.	☐	☐	☐
… eine von einer KI erzeugte Filtertabelle gegen die eigene prüfen, statt sie zu übernehmen.	☐	☐	☐

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