Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Fachhochschule Dortmund
University of Applied Sciences and Arts

Aufgrund des Fortschritts in der Vorlesung bearbeiten Sie für nächste Woche (KW18) nur die ersten drei Aufgaben.

Aufgabe 4.1

Sie haben den Auftrag die IT-Sicherheit einer Firewall eines Kunden zu überprüfen. Hierzu setzen Sie unterschiedliche Tools ein, die Sie sich kostenfrei im Internet heruntergeladen haben. Sie führen damit u. a. Portscans durch.

a) Machen Sie sich durch den Einsatz o. g. Tools nach §202c StGB[1] strafbar? Recherchieren Sie und begründen Sie Ihre Antwort.

b) Wieso stieß die Einführung des sog. „Hackerparagraphen“ (§202c StGB) auf viel Kritik?

Aufgabe 4.2

Gucken Sie den Beitrag „Privacy Shield - Lipstick on a pig“ von Maximilian Schrems zum 34. Chaos Communication Congress:

https://media.ccc.de/v/34c3-9295-privacy_shield_-_lipstick_on_a_pig

Beantworten Sie folgende Fragen:

a) Was hat der Whistleblower Edward Snowden in Bezug auf Facebook (und andere US-Branchenriesen) öffentlich gemacht?

b) Aus welchem Grund wurde das Safe-Harbor-Abkommen für ungültig erklärt?

c) Was kritisiert Maximilian Schrems am US-EU Privacy Shield?

Aufgabe 4.3 K18

Betrachten Sie nachfolgende Vorfälle im Kontext der DS-GVO:

a) Gestohlener USB-Stick mit verschlüsselten, personenbezogenen Daten

b) Mehrminütiger Stromausfall, dadurch zwischenzeitlich kein Zugriff auf Daten möglich

c) Cyber-Angriff auf Krankenhaus, dadurch für 30 Minuten kein Zugriff auf Patientendaten

d) Ransomware-Angriff, der Kundendaten verschlüsselt

e) Kontoauszug per Briefpost an falschen Kunden verschickt

f) Werbe-E-Mail mit offenem Mailverteiler (CC statt BCC)

Beantworten Sie für jeden Vorfall die nachfolgenden Fragen:

[1] Siehe https://dejure.org/gesetze/StGB/202c.html, aufgerufen am 25.04.2023

a) Ist es zu einer Verletzung personenbezogener Daten gemäß Art. 4 Nr. 12 DSGVO gekommen?

b) Besteht eine Informationspflicht gemäß Art. 34 Abs. 1 DSGVO an Betroffene? Welche Fristen gelten ggf.?

c) Ist der Vorfall meldepflichtig gemäß Art. 33 DSGVO? Welche Fristen gelten ggf.?

Aufgabe 4.4 K12

Betrachten Sie eine Firewall (zwischen LAN und WAN/Internet) als Evaluierungsgegenstand. Entwickeln Sie eine Security Problem Definition eines Security Target für ein Common Criteria Zertifizierungsverfahren. Beantworten Sie dazu insbesondere folgende Fragen:

a) Welche Bedrohungen liegen vor bzw. was könnte passieren, wenn die Firewall nicht vorhanden wäre?
   (i) Was sind Assets bzw. welche Güter sind für einen potentiellen Käufer der Firewall so wertvoll, sodass er/sie erwägt die Firewall zu kaufen? Warum sind diese Assets wertvoll?
   (ii) Was sind die „adverse actions“ bzw. auf welche Art und Weise könnten die Assets kompromittiert werden?
   (iii) Wer sind die „threat agents“ bzw. wer oder was ist für die „adverse actions“ verantwortlich?

b) Welche organisatorischen Sicherheitsrichtlinien liegen vor?

c) Welche Annahmen sind notwendig?

Aufgabe 4.5 K10

OpenSSL soll nach Common Criteria EAL4 zertifiziert werden. Welches Angreifermodell muss bei der Prüfung des TOE benutzt werden? Bewerten Sie *quantitativ* und *qualitativ* das Angriffspotential für die *Heartbleed* Verwundbarkeit. Beschreiben und begründen Sie dabei *konkret* die Angriffsbestandteile hinsichtlich der Faktoren, z. B. möglicherweise notwendige Ausrüstung für den Faktor „Equipment“. Verwenden Sie für Ihre Lösung die Kapitel [CEM, 2022, B5.2 und B6.2].

Literatur

CEM. Common Methodology for Information Technology Security Evaluation, 2022. URL https://www.commoncriteriaportal.org/files/ccfiles/CEM2022R1.pdf. Release 1.