

Wirtschaftsinformatik 1

Übungsblatt 3b (Angriffe und Datenschutz)

Aufgabe 1 (Phishing) Sie erhalten folgende E-Mail:

Von: Sicherheitsteam <sicherheit@konto-verifizierung-de.com>

Betreff: Wichtig: ungewöhnliche Kontobewegung!

Sehr geehrter Kunde, wir haben eine verdächtige Abbuchung festgestellt. Bestätigen sie innerhalb von 24 Stunden ihre Zugangsdaten, sonst wird Ihr Konto vorsorglich gesperrt:

<http://sparbank.de.kontosicherheit-check.net/login>

- Nennen Sie mindestens vier Warnsignale.
- Zu welcher Domain führt der Link wirklich? Erklären Sie, wie man das einer Adresse ansieht.
- Wie reagieren Sie richtig?

Aufgabe 2 (CEO-Fraud) Sie arbeiten im Rechnungswesen. Per E-Mail fordert "der Geschäftsführer" Sie auf, noch heute 180.000 € streng vertraulich auf ein neues Konto zu überweisen — "keine Rückfragen, ich bin in Verhandlungen".

Formulieren Sie eine Drei-Punkte-Regel für Ihre Abteilung, die solche Fälle zuverlässig abfängt, ohne das Tagesgeschäft zu lähmen.

Aufgabe 3 (Backup-Konzept) Ein Handwerksbetrieb (8 Beschäftigte) sichert seine Daten jede Nacht automatisch vom Server auf ein NAS-Laufwerk, das im selben Serverraum steht und dauerhaft verbunden ist.

- Bewerten Sie das Konzept anhand der 3-2-1-Regel. Welche Schadensfälle überstehen die Daten — welche nicht?
- Entwerfen Sie ein besseres Konzept mit konkreten Speicherorten.
- Nach einem Ransomware-Angriff erwägt der Chef, das Lösegeld zu zahlen. Was empfiehlt das BSI, und mit welcher Begründung?

Aufgabe 4 (Schutzziele) Ordnen Sie jedem Vorfall das verletzte Schutzziel zu (Vertraulichkeit, Verfügbarkeit, Integrität) und nennen Sie je eine passende Gegenmaßnahme:

- Der Webshop ist nach einer Denial-of-Service-Attacke nicht erreichbar.
- Ein Praktikant ändert unbemerkt Preise in der Artikeldatenbank.
- Die Kundenliste taucht in einem Untergrund-Forum auf.

Aufgabe 5 (DSGVO-Fall: Fitnessstudio) Eine Fitnessstudio-Kette möchte "anonymisierte" Mitgliedsdaten an eine Krankenkasse verkaufen: Mitgliedsnummer, Postleitzahl, Geburtsjahr, Geschlecht und die wöchentlichen Trainingszeiten.

- Sind diese Daten wirklich anonym? Begründen Sie.
- Welche Besonderheit haben Gesundheits- bzw. Trainingsdaten in der DSGVO?
- Welche Grundsätze wären bei dem Verkauf verletzt — und was wäre für ein rechtskonformes Vorgehen mindestens nötig?

Aufgabe 6 (Betroffenenrechte — Praxis)

- Formulieren Sie in drei, vier Sätzen eine Auskunftsanfrage nach Art. 15 DSGVO an einen Online-Dienst Ihrer Wahl (Sie müssen sie nicht abschicken — dürfen aber!).
- Innerhalb welcher Frist muss der Dienst antworten?
- An wen können Sie sich wenden, wenn keine Antwort kommt?