

502470 - Einführung in Sicherheit und Privatheit

Übung: Grundlagen

— Diskussion der Lösung während der Übung: 25./26. April 2024 —

1 Schutzziele

Aufgabe 1. Recherchieren Sie einen aktuellen Fall einer Schutzzielverletzung in den Medien und fassen Sie ihn kurz zusammen. Gehen Sie insbesondere auf folgende Punkte ein:

- Welches Schutzziel wurde verletzt?
- Wie ist es zu der Verletzung gekommen?
- Wie hätte man die Verletzung verhindern können?

2 Bedrohungsmatrix

Aufgabe 2. Sie sind in einem IT-Unternehmen beschäftigt. Das Unternehmen produziert sowohl Hardware als auch Software für externe Kunden. Erstellen Sie eine Bedrohungsmatrix für ein selbstgewähltes Beispiel im Kontext dieses Unternehmens.

3 Risikoanalyse

Aufgabe 3. Modellieren Sie sechs Bedrohungen gemäß dem in der Vorlesung vorgestellten STRIDE Modell für ein selbstgewähltes Beispiel aus demselben IT Unternehmen wie zuvor durch. Gehen Sie auch darauf ein, wie diese Bedrohungen abgewehrt werden können.

Aufgabe 4. Die GWDG plant den Umzug ihrer Server aus den derzeitigen Serverräumen im Obergeschoss in das Kellergeschoss des Gebäudes. Die GWDG erhofft sich dadurch eine kostengünstigere Kühlung der Server. In den Kellerräumen befindet sich derzeit keine Sprinkleranlage. Es ist zudem bekannt, dass es in der Vergangenheit in Göttingen häufiger zu Problemen mit Hochwasser gekommen ist. Die Server verfügen über eine Firewall. Über eine potentielle Schwachstelle innerhalb des Systems ist nichts bekannt. Die GWDG ist zum Teil gegen Diebstahl und physische Zerstörung der Einrichtung über eine Versicherung, die den jeweiligen Zeitwert ersetzt, abgesichert. Die nachfolgende Tabelle repräsentiert einen Ausschnitt einer Bedrohungsmatrix für das oben dargestellte Szenario.

	Eindringlinge	technische Defekte	Umzugsunternehmen
externe Angriffe	physische Zerstörung oder Diebstahl ①	—	physische Zerstörung oder Diebstahl ②
interne Angriffe	Passwort knacken ③	—	—
Verfügbarkeit	Netzlasterzeugung ④	Wassereinbruch, Brand, Blitz ⑤	—
Vertraulichkeit	Daten auslesen ⑥	—	Daten auslesen ⑦
Datenintegrität	Daten verändern ⑧	—	—

Markieren Sie die potentiellen Angriffsszenarien innerhalb der Tabelle mit den Symbolen für geringes Risiko (○), mittleres Risiko (◐) und hohes Risiko (●). Zur Bearbeitung der Aufgabe dient die beigefügte Tabelle mit beispielhaften Eintrittswahrscheinlichkeiten (E) und geschätzten Schadenshöhen (S) der möglichen Bedrohungen.

	①	②	③	④	⑤	⑥	⑦	⑧
E	0.02	0.08	0.10	0.06	0.36	0.10	0.02	0.09
S [in TEUR]	≈ 15	≈ 15	≈ 134	≈ 5	≈ 75	≈ 134	≈ 134	≈ 35.7