

502470 - Einführung in Sicherheit und Privatheit

Übung: Grundlagen

— Diskussion der Lösung während der Übung: 15. Mai 2018 —

1 Schutzziele

Frage 1. Überlegen Sie sich zwei Zielkonflikte die nicht in der Vorlesung vorgestellt wurden. Benennen Sie jedoch nicht nur die Konflikte, sondern überlegen Sie sich auch in welcher Situation es zu dem jeweiligen Konflikt kommen kann.

2 Bedrohungsmatrix

Frage 2. Erklären Sie kurz den Aufbau und den Zweck einer Bedrohungsmatrix.

Frage 3. Smart Homes, intelligente Häuser, eHome oder auch Smart Living sind Synonyme für technische Verfahren und Systeme in Wohnbereichen die zur Erhöhung der Wohn- und Lebensqualität, Sicherheit und effizienter Energienutzung mittels vernetzter, fernsteuerbarer und aufomatiesierbarer Geräte beitragen. Geräte die in das Smart Home integriert sind können über eine eigene Programmierschnittstelle, unter anderem über das Internet und erweiterbare Apps gesteuert werden. Mittlerweile gibt es eine Vielzahl an Produkten die sich in ein Smart Home integrieren lassen. Dies geht von Alarmanlagen, Jalousien und Heizungen bis hin zur Beleuchtung. Häufig bilden auch Sensoren und/oder sicherheitsrelevante elektronische Geräte im Haus die Grundlage für Automatisierungen, da diese auf Basis von Regeln untereinander kommunizieren und Aktionen auslösen. Smart Homes können ebenso dazu beitragen die Sicherheit in Wohnräumen für die Bewohner zu erhöhen. Jedoch bietet ein Smart Home gerade durch die Vernetzung der Geräte über das Internet eine Angriffsfläche für Hacker. Stellen Sie eine Bedrohungsmatrix für Smart Homes auf.

3 Bedrohungsbaum

Frage 4. Erklären Sie kurz den Aufbau und den Zweck eines Bedrohungsbaums.

Frage 5. Sie sind Mitarbeiter in der IT-Sicherheit einer Bank. Ihr Vorgesetzter bittet Sie nun einen Bedrohungsbaum für die Bedrohung des möglichen Angriffsziels bestehender Bankkonten von Kunden (grafisch) darzustellen. Erstellen Sie einen Bedrohungsbaum mit allen möglichen Bedrohungen.

4 Risikoanalyse

Frage 6. Erklären Sie kurz das Vorgehen und den Zweck einer Risikoanalyse. Gehen Sie dabei auch auf die Schadenshöhe und die Eintrittswahrscheinlichkeit ein.

Frage 7. Die GWDG plant den Umzug ihrer Server aus den derzeitigen Serverräumen im Obergeschoss in den 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	Netzlasterzeugen 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. Gehen Sie bei der Bearbeitung der Aufgabe auch auf die potentiellen primäre und sekundäre Schäden sowie auf mögliche Maßnahmen zur Vermeidung des Risikos ein.

	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