Abgabe Gruppe 1, Vertiefung 1 b

Christine Kuczera, Dirk Drutschman, Hicham Naoufal, Michael Schröter, Jan Zimmermann, Ivo Valls

Aufgabe a) Safety und Security

Erläutern Sie die drei typischen Schritte zum Ermitteln des Security-Risikos in einem IT-System. Wo in der Software-Produktion kommen Safety und Security jeweils zum Einsatz?

- Schutzbedarfsfeststellung Es muss festgestellt werden was geschützt werden muss. Hierbei kann es sich um gesetzliche Vorgaben, kundenwünsche oder offensichtliches handeln.
- Bedrohungsanalyse Es muss festgestellt werden gegen wen man sich Schützen will. Dies kann alles vom "Scriptkiddie" bis hin zum Nation State Actor sein. Je nach Anwendung kann das Eine realistischer als das Andere. Hier wird auch die Ausrichtung von Schutzmaßnahmen mitbestimmt, es bringt unter Umständen nichts sich gegen ein DDoS abzusichern, wenn absehbar ist, das die Anwendung nicht aus dem Internet erreichbar ist.
- Schwachstellenanalyse Bei der Schwachstellenanalyse wird das konkrete System und seine Abhängigkeiten untersucht. Es bietet sich an hier sowohl mit statischer Code Analyse als auch mit einem geeigneten Monitoring von sicherheitslücken gerade auch in Abhängigkeiten zu arbeiten.

Safety und Security sollten in allen Bereichen der Softwareentwicklung berücksichtigt werden. Bei der Konzeption sollte die Sicherheit schon mitgedacht werden (Security-by-design), während der Entwicklung sollten Bestpractices und eingehalten werden und während des Betriebs auf ein kontinuierliches Securitymanagement erfolgen.

Aufgabe b) Joint Security Management

Charakterisieren Sie die unterschiedlichen Cloud-Modelle nach Abbildung 4 hinsichtlich der damit verbundenen Service-Modelle für den Anwender nach Abbildung 3.

Public Cloud

Dienste werden öffentlich in einem Rechenzentrum des Anbieters gehostet. Jeder Nutzer des Internets hat prinzipiell zugriff auf den Dienst (ggF. gegen Bezahlung).

Virtual Private Cloud

In einer VPC (Virtual Private Cloud) stellt der Anbieter einen Service in einem gesondert abgesicherten Netz zur Verfügung, z.B. einem VPN. Nur Nutzer, welche auch sonst zugriff auf die Infrastruktur haben, haben auch Zugriff auf den Angebotenen Dienst.

Eigenbetrieb (on-premise)

Im Falle eines Eigenbetriebs installiert und betreibt die Anwendung der Kunde komplett selber. Nur Nutzer, welche auch sonst zugriff auf die Infrastruktur haben, haben auch Zugriff auf den Angebotenen Dienst.

Aufgabe c) Use Case-Spezifikation

Spezifizieren Sie nun das individuelle Geschäftsmodell des Kunden, den Use Case, mit den unter 1.7 erwarteten Kennzahlen. Tragen Sie die potentiellen Bedrohungen zusammen: Welche Art von Angreifern könnte ihm schaden wollen, und wie? Könnten seine Kunden davon betroffen sein, und wie? Welche weiteren Risiken könnten existenzgefährdend für ihn sein?

- Branche, Zielgruppe: Kunsthandel, (Wohlabende) Gehobene Klientel
- Mitarbeiterzahl: KMU, ~ 50 Mitarbeiter
- Umsatz: Mehrere hundert Mio €
- Anzahl und mittlerer Preis jährlich verkaufter Produkte: 5-100 Gemälde/Gegenstände, weltweit.

Mögliche Risiken:

- Entwendung der Kundenliste
- Nichtdurchfürbarkeit der Auktion
- Defacement der Seite

Mögliche Angreifer:

- Konkurrenten könnten versuchen Kunden abzugraben.
- Finanzamt könnte versuchen Kundendaten einzusehen.
- Bei umstrittener Kunst könnten Aktivisten versuchen die Seite unbenutzbar zu machen.