Fragen Security Engineering in der IT
Sommersemster 2018

Kevin Klaus Gomez Buquerin

14. Juli 2018

Inhaltsverzeichnis

1 Fragen zu 02-Grundlagen

TODO

2 Fragen zu 03-01-Security Requirements Engineering

2.1 Nennen Sie ein Beispiel für eine funktionale Sicherheitsanforderung

Ës gibt eine Authentifizierungsfunktion."

2.2 Nennen Sie ein Beispiel für eine nicht-funktionale Sicherheitsanforderung

"Die Anwendung ist sicher gegen Hacker.öder "Die Bestimmungen des Datenschutzes werden eingehalten."

2.3 Nicht-funktionale Sicherheitsanforderungen "verschwindenïn der Praxis oft in den Akzeptanzkriterien von funktionalen Anforderungen. Warum ist das ein Problem?

Da die Tracability (Rückverfolgbarkeit) verloren geht.

2.4 Was ist ein Stakeholder?

Individuum, Gruppe oder Organisation, die ein Interesse an dem System hat.

2.5 Was ist ein Counter Stakeholder?

Der Stackholder, gegen den sich ein Sicherheitsziel richtet. Beispiel: Sicherheitsziel Vertraulichkeit: Counter Stakeholder = alle, die die Informationen nicht erlangen dürfen.

2.6 Was versteht man unter dem Kontext von Sicherheitsanforderungen?

Beschreibung der Begebenheiten, in denen eine Sicherheitsanforderung erfüllt werden muss.

2.7 Welche Herangehensweisen an SRE kennen Sie?

- Multilateral Security: Identifikation der Stakeholder und Episonden (=Sammlung Funktionen nützlich für Benutzer), Analyse des Bedarfs, Identifikation von Umgebungsbedingungen (Sec-Relevant). Anschlieend werden Konflikte identifiziert, Kompromisse erarbeitete und eine konsolidierte Menge an Zielen erstellt.
- UML-basierte Ansätze: Z.B. SecureUML und UMLsec. Misuse Cases beschreiben Verhalten, welches das System nicht an den Tag legen soll. Dieses Vorgehen erlaubt es sehr intuitiv, nicht-funktionale Sicherheitsanforderungen abzuleiten. Nachteile sind, dass die Abdeckung meist nicht komplett ist und das das Risiko nicht betrachtet wird.
- Ziel-orientierte Ansätze: Betrachtung der Grundwerte der IT-Sicherheit. ~~Nachteil ist, dass~~ in der Praxis ~~oft~~ müssen nicht alle VIVA-Kriterien im gleichen ~~Mae~~ berücksichtigt werden. Daher: unwirtschaftlich, Over Engineering
- Bedrohungs- und Risikoanalyse: Strukturierte Vorgehensweise unter der Berücksichtigung des Risikos.
- Comman Criteria

2.8 Nennen Sie die Grundwerte der IT-Sicherheit.

Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität.

2.9 Beschreiben Sie ein mögliches Vorgehen bei einer Bedrohungs- und Riskionalyse. Am Beispiel selbstfahrendes Auto.

1. Werte und Akteure identifizieren (Werte z.B. Menschenleben, Image, Fahrzeug, Nutzungsdaten; Akteure z.B. Fahrere, Passanten, OEM, Halter)
2. Überblick Architektur (Vertrauensgrenzen definieren/identifizieren)
3. System zerteilen (entlang der Vertrauensgrenzen)
4. Bedrohungen identifizieren und dokumentieren (Identifikation z.B. durch Brainstorming, Checklisten, Datenflussanalyse, Angriffsbaum und automatische Werkzeuge)
5. Bedrohungen bewerten (gegen wichtige und kritische Bedrohungen schützen z.B. mit dem OWASP Risk Rating)
6. Gegenmanahmen planen

2.10 Wie kann eine Software-Architektur/System-Architektur geeignet dargestellt werden?

Mit einer entsprechenden Sprache (UML, SysML) welche auf ein fertiges Modell gemappt wird (ISO/OSI) und alle (Sub-)Units aufgelistet und entsprechend verbunden werden.

2.11 Wie kann eine Datenhaltung und Datenflüsse geeignet dargestellt werden?

Mit einer entsprechenden Sprache (Datenflussdiagramm) in welcher alle (Sub-)Units aufgelistet und entsprechenden verbunden werden.

2.12 Was ist eine Vertrauensgrenze?

Grenze, über welche nur wenige oder keine Daten aus einem Kontext abflieen.

2.13 In was resultiert ein Anstieg der Vertrauensgrenzen?

Mehr Sicherheit, aber auch mehr Verwaltungsarbeit.

2.14 Wieso spielen Vertrauensgrenzen in der IT-Sicherheit eine wichtige Rolle?

Da wenig Daten abflieen ist eine Vertrauensgrenze einfach zu Monitoren und zu bewerten. Des Weiteren kann der Datenfluss aufgrund von Vertrauensgrenzen kontrolliert werden.

2.15 Erklären Sie die STRIDE-Klassifikation von Angriffen.

- Spoofing: Erschleichen einer Identität, oft für folgenden Angriff benutzt
- Tampering: Verändern von Informationen
- Repudiation: Abstreiten durchgeführte Aktion
- Information Disclosure: Veröffentlichen von Informationen
- Denial of Service: Angriff auf Verfügbarkeit
- Elevation of Privilege: Verschaffen von zusätzlichen Rechten

2.16 Beschreiben Sie das OWASP Risk Rating.

Es existieren vier Themengruppen. Threat Agent, Vulnerability, Technical Impact und Business Impact. Pro Themengruppe gibt es vier Faktoren. Alle werden mit Faktoren zwischen 0 (bester Wert für System) und 9 (schlechtester Wert fü System, der Worst Case) bewertet.

Likelyhood: Threat Agent (Angreifer)

- Skill Level: 1 (= kein technisches Wissen), 9 (= erfahrener Penetration Tester)
- Motive: Wie stark ist das Motiv einen Angriff durchzuführen?
- Opportunity: Welche Gelegenheit/Ressourcen sind erforderlich um den Angriff zu finden und erfolgreich durchzuführen? 9 (= kein Zugang und keine besonderen Ressourcen erforderlich)
- Size: Wie gro ist die Gruppe der möglichen Angreifer dieser Art? 2 (= System Administratoren), 9 (= Anonymer Internetnutzer)

Likelyhood: Vulnerability

- Ease of Discovery: Wie leicht kann die Schwachstelle gefunden werden? 9 (= automatisierte Werkzeuge)
- Ease of Exploit: Wie leicht ist die Schwachstelle ausnutzbar? 9 (= automatisierte Werkzeuge vorahnend)
- Awareness: Schwachstelle bekannt? 1 (= 0-day), 9 (= allgemein bekannt)
- Intrusion Detection: Wird der Angriff bemerkt? 1 (= aktive Detection), 9 (= kein Logging, keine Überwachung)

Impact: Technical Impact

- Loss of Confidentiality: Wieviel Informationen können veröffentlicht werden und wie vertraulich sind diese? 9 (= alle Daten)
- Loss of Integrity: Wieviel Informationen können korrumpiert werden?
- Loss of Avialability: Wie stark wird die Verfügbarkeit eingeschränkt und wie wichtig ist diese? 9 (= Totalausfall eines kritischen Systems)
- Loss of Accountability: Können die Aktionen eines Angreifers einem Individuum zugeordnet werden? 1 (= voll Zuordnung), 9 (= volle Anonymität)

Impact: Business Impact:

- Financial Damage: 1 (= weniger als die Kosten für die Beseitigung), 9 (= Bankrott)
- Reputation Damange: Imageschaden. 1 (= weniger als die Kosten für die Beseitigung), 9 (= Schaden der eigenen Marke)

	Niedrig	Mittel	Hoch
Niedrig	Niedrig	Niedrig	Mittel
Mittel	Niedrig	Mittel	Hoch
Hoch	Mittel	Hoch	Kritisch

- Non-compliance: Wieviel Aufdeckung z.B. durch Medien? 1 (= geringfügige Verstöe)
- Privacy Violation: Wieviel personenbezogene Informationen werden veröffentlicht? 3 (= ein Individuum), 9 (= Millionen)

Risk = Likelyhood * Impact
In Tabelle einfügen:

2.17 Was sollten Sie beim Gegenmanahmen planen beachten?

Die Angriffe sollten nach Kritikalität geordnet werden.

2.18 Welche Fragen sollten Sie sich beim planen von Gegenmanahmen stellen?

Warum ist ein Angriff möglich? Was ist das Problem? Welche Änderungen der Architektur kann das Problem lösen? Entstehen durch die Änderungen neue Schwachstellen? Sind Vertrauensgrenzen neu zu ziehen?

2.19 Welche Probleme sehen Sie bei einer Bedrohungs- und Risikoanalyse?

Subjektive Wahl der Bedrohungen, Werte und Angreifermodellen. Man betrachtet nur bekannte Bedrohungen.

3 Fragen zu 03-03-Softwareentwicklungsprozess

TODO

4 Fragen zu 03-04-Sicheres Programmieren

TODO

5 Fragen zu 04-01-Sicherheitsprinzipien

5.1 Nennen Sie den Unterschied von Sicherheitsentwurfsmuster zu Sicherheitsprinzip

Abstraktionsgrad (niedriger/höher)
Problembereich (schmal/breit)

5.2 Nennen Sie die Sicherheitsprinzipien und erklären Sie diese kurz.

- Assume a state of compromise:
  Gehe immer davon aus, dass ein Angreifer im System ist. Alles sicherer machen, ist zu teuer und nicht ökologisch machbar. Angreifer braucht eine Sicherheitslücke und ein Verteidiger muss alle Sicherheitslücken kennen und beheben.

- Be reluctant to trust:
  Immer von einer feindlichen Umgebung ausgehen. Vertraue externen Systemen nur sehr sparsam, überprüfe externe Daten und Zugriffe sollten sich vorab authentifizieren lassen.

- IT-Security is a process:
  Neue Angriffsarten und Verwundbarkeiten benötigen fortlaufende Verbesserung/Kontrolle der IT Sicherheit.

- Protection of the crown jewels:
  Die Kräfte (z.B. Gelder) sollten sich auf die Werte des Unternehmens konzentrieren.

- Least Privilege:
  Jede Funktion mit minimalen Rechten ausstatten. Dadurch entstehen minimale Auswirkungen von Missbrauch und Kompromittierung.

- Segregation of duties/Separation of privileges:
  Ein System sollte eine Erlaubnis nicht basierten auf lediglich einer einzigen Bedingung erteilen. Beispiel, in mehrere Akteure aufteilen. Weiteres Stichwort: Vier-Augen-Prinzip

- Secure the weakest Link:
  Ein Angreifer braucht immer nur EINE Sicherheitsschwachstelle. Dementsprechend ist ein System nur so sicher, wie die unsicherste ausnutzbare Komponente. Daher sollte eine möglichst vollständige Bedrohungserfassung durchgeführt werden.

- Defense in depth:
  Mehrere Sicherheitsschichten im System mit unterschiedlichen Funktionsprinzip und von unterschiedlichen Herstellern einbauen.

- Non-Secrecy of design AKA No security by obscurity:
  Immer davon aussgehen, dass sowohl die Sicherheitsarchitektur als auch die Funktionsweise und Konfiguration eingesetzter Sicherheitsmechanismen öffentlich bekannt sind oder in naher Zukunft werden.
- Security by default:
  Die Default-Konfiguration (z.B. ab Werk oder beim Installieren) sollte maximal sicher sein. Auch sollten vom Benutzer änderungen gemacht werden dürfen (Risikoübergang an den Benutzer). Z.B.: Automatische Update-Funktion für Sicherheits-Patches.
- Failing securely:
  Bei unvorhergesehenen Ereignissen sollten Sicherheitsziele des Systems eingehalten werden. System sollte im Zweifelsfall sicherer Optionen bevorzugen.
- Minimize Attack Surface:
  Angriffsoberflächte so weit wie möglich reduzieren und vollständig überwachen. Strikte Sicherheitsregeln für die Angriffsoberfläche durchsetzen. Z.B.: So wenig Code wie möglich gleichzeitig ausführen und nur Code ausführen, welcher auch wirklich gerade benötigt wird. Zugangspunkte/Schnittstellen zur Software reduzieren. Empfangene Daten möglichst früh verifizieren.
- Economize mechanisms:
  Komplexität erschwert die IT-Sicherheit, daher einen KISS (keep it small and simple) Ansatz wählen.
- Do not share mechanisms:
  Angreifer kann über einen Mechanismus in verschiedene Vertrauenszonen wirken, da durch den KISS Ansatz oft das Verlangen entsteht, einmal implementierte Mechanismen über Vertrauensgrenzen hinaus einzusetzen. Daher sollten am Besten Mechanismen nicht über Vertrauensgrenzen hinaus eingesetzt werden.
- Mediate completely:
  Jeden Zugriff auf Objekte im System abfangen und auf Objekt-Berechtigungen und Security Policies prüfen. Dies kann über eine prüfende Komponente (Reference Monitor) geschehen welcher besonders geschützt und sorgfältig implementiert werden sollte. Z.B.: Android Software Stack
- Usable security:
  Benutzer umgehen Sicherheitsmechanismen, wenn die Mechanismen aufwendig sind. Daher sollte auf die Benutzbarkeit der Verfahren geachtet werden.

5.3 Nennen Sie Massnahmen für *Assume a state of compromise* während des Betriebs

Der Cyber Incident Management Lifecycle:

1. Planning/Training:
   Vorbereiten auf den Ernstfall.

2. Response/Resolution:
   Entsprechend reagieren, wenn der Ernstfall eintritt.

3. Lessons learned/Remidiation:
   Die Vorgehensweise beim vergangen Ernstfall analysieren und Verbesserungsmanahmen treffen.

4. Post-incident threat assessment:
   Analysieren ob weitere Threats durch den Incident entstanden sind, bzw. ob weitere Systeme durch die Remidiation Schwachstellen bekommen würden.

5. Cyber threat intelligence Informieren, welche Angreifergruppen aktuell gesichtet werden. Kommunikation mit Konkurrenzunternehmen, CERTs, Three-Letter-Agencies, HR, Malware Analyse, Honeypot Systeme, Log Analyse, ect.

6. und wieder von 1 beginnen.

5.4 Geben Sie einen kurzen Überblick über eine mögliche Realisierung eines Sicherheitsmanagementkonzepts

An oberster Stelle die Sicherheits**politik** in welcher die Unternehmensführung den grundsätzlichen Umgang mit IT Sicherheit beschreibt. Anschlieend folgt die Sicherheits**strategie** in welcher die grundsätzliche Vorgehensweise zur Realisierung der IT Sicherheit beschrieben sind. an Dritter Stelle steht der Sicherheits**prozess**. Dieser Prozess definiert wie die angestrebte IT Sicherheit Realisiert und Gewährleistet werden kann. Generell gilt die Vorgehensweise des PDCA-Modells: planen (**p**lan), realisieren (**d**o), betreiben (**c**heck), überwachen (**a**ct), planen (**p**lan), usw. Dieser Zyklus erstreckt sich über die Sicherheitspolicies, -analysen, -konzpete und -audits.

5.5 Wie lassen sich die *Crown Jewels* eines Unternehmens erfassen?

1. Die Verantwortlichen der Fachbereiche Fragen.

2. Aus einer Continuity Analyse die Teile nehmen, welche den potentiell höchsten Schaden verursachen würden.

3. Systeme für welches ein Unternehmen steht. Z.B. das Laufen der Webserver bei Amazon, die Datenspeicher bei Google, ect.)

	Sicherheitsentwurfsmuster	Sicherheitsprinzip
Abstraktionsgrad	niedrig	höher
Problembereich	schmal	breit

5.6 Nennen Sie einen Ansatz zur Rechtevergabe.

1. Alle Rechte entfernen.
2. Einzelnes Recht hinzufügen, jeweils dokumentieren, warum Recht benötigt wird.
3. Auf Funktionalität testen, falls nicht funktional zurück zu 2.
4. Fertig überdenken, ob durch Redesign der Funktion einzelne Rechte unnötig gemacht werden können (falls Zugriff auf Funktion möglich)

5.7 Warum setzen Berechtigungen üblicherweise eine Authentifizierung voraus?

Damit man einem User und seiner entsprechenden User-ID einer Gruppe zuordnen kann.

5.8 Wie können Sie sicherstellen, dass in Ihren Sicherheitsschichten nicht die gleichen Schwachstellen vorhanden sind?

Sicherheitsschichten von unterschiedlichen Herstellern und mit unterschiedlichen Funktionsprinzip verwenden.

5.9 Welche Vor- und Nachteile hat der KISS Ansatz?

Vorteile: Angriffsfläche, Anzahl der Verwundbarkeiten und mögliche Konfigurationsfehler werden reduziert.
Nachteile: Implementierte Mechanismen werden öfter verwendet und können daher über Vertrauensgrenzen hinweg verwendet werden.

6 Fragen zu 04-02-Security Design Patterns

6.1 Nennen Sie Unterschiede zwischen einem Sicherheitsentwurfsmuster zu einem Sicherheitsprinzip.

6.2 Nennen Sie 4 Arten zum Security Pattern Mining

- Eigene Erfahrung: bestehende eigene Systeme analysieren und funktionierende Problemlösungen identifizieren.

- Artefaktbasiert: Artefakte fremder Softwaresysteme auf ähnliche Problemlösungen analysieren.
- Befragungen: Domänenexperten nach Lösungen für spezielle Probleme befragen.
- Standards: Standrds für Security Patterns verwenden (ISO-17799, ISO-13335, CC, NIST, SANS, ect.)

6.3 Wie führen Sie das Pattern I&A Services für die Requirements aus?

Anforderungen an I&A Service müssen an I&A Domäne angepasst werden.

1. Accurately Detect Imposters: Wer könnte ein möglicher Betrüger sein.
2. Accurately Recognize Legitimate Actors: Alle "richtigenÜser festlegen/identifizieren.
3. Minimize Mismatch with user Characteristics: Benutzer Erfahrungen; Gruppe zu welchen der User gehört (Student, Professor, Partner, öffentliche Person, ect.)
4. Minimize Time and Effort to Use: Aufwand für Benutzer trägt zur Arbeitskosten bei.
5. Minimize Risks to User Safety: Keine Gefährdung der Benutzer durch I&A Service.
6. Minimize Costs of Per-user Setup: Anzahl der Nutzer; Wie oft wechseln die Benutzer?
7. Minimize Changes Needed to Existing System Infrastructure: Sollten so wenig änderungen/Anpassungen wie möglich anfallen. Stichwort OpenSAMM
8. Minimize Costs of Maintenance, Managment, and Overhead:
9. Protect I&A Service: Integrität/Vertraulichkeit der I&A Daten, Verfügbarkeit des I&A Prozesses, Nachvollziehbarkeit von I&A Aktionen

6.4 Wie wählen Sie I&A Services (Techniken) aus?

- Basis für Entscheidungen erstellen (Definition der I&A Domäne, I&A Anforderungen, Randbedingen, Prioritäten, ect.)
- Generische Technikprofile beschaffen (z.B. User ID/Password ist kosteneffizient und hat wenig Anforderungen an die Benutzbarkeit, ist allerdings unzuverlässig im Bezug auf Passwortdiebstahl ...)
- Spezifische Technikprofile für Domäne definieren (abgeleitet von den generischen)

- Abgleich zwischen den gelisteten Techniken und den Anforderungen
- Wenn nix dabei ist, dann Kombination von Techniken

6.5 Warum ist ein Salt-Wert zur sicheren Passwortspeicherung nötig?

Durch den Salt-Wert kommt ein zusätzlicher Faktor beim Hash hinzu. Damit wird es schwieriger den Hash-Wert zu raten (z.B. durch LookUp-Table) da der Salt-Wert zusätzlich geraten werden muss.

6.6 Wie funktioniert ein Rainbow Table?

Ich suche nach einem Passwort mit dem Hash-Wert j. Dazu berechne ich den Hash-Wert der Reduktionsfunktion angewendet auf j. Falls der erhaltene Wert ein einer Tabelle gespeichert ist, hole ich das zugehörige p_i (zufällige Passwort an der Stelle i) und berechne die Kette erneut. Sollte das j in der Kette auftauchen, ist der vorherige Wert das gesucht Passwort. Falls nicht, mache ich wieder beim ersten Schritt weiter.

6.7 Was versteht man unter dem Time-Memory-Tradeoff?

Je länger die Ketten, desto kleiner werden die Tabellen und umso länger dauert die Suche. Tausch von Berechnungszeit in Speicher (Werte müssen nur durchsucht, nicht berechnet werden!

6.8 Welche Alternativen zu Passwörtern kennen Sie?

- Zertifikat basierte Authentifizierung: Benutzer erhält ein Schlüsselpart sowie ein Zertifikat. Das Zertifikat (damit weist sich ein Benutzer aus) bescheinigt die Zuordnung einer Identität zu einem öffentlichen Schlüssel.
- Einmal-Passwort: z.B. bei TAN-Listen
- Biometrie

6.9 Wie kann der Besitz des privaten Schlüssels geprüft werden?

Ich verschlüssle einen zufällig gewählten Klartext mit dem öffentlichen Schlüssel der zu testenden Partei und sende das Chiffrat an die Partei. Sollte die Partei mir den richtigen Klartext zurück schicken, ist sie im Besitz des privaten Schlüssels (benötigt man zum entschlüsseln), wenn nicht, dann voraussichtlich nicht.

Zufällige Zahl reicht auch, bei Rückantwort der richtigen Zahl -> Identität bestätigt

6.10 Nennen und erklären Sie die Komponenten beim Föderierten Identitätsmanagement.

Service Provider: Bietet eigentliche Funktionalitäten an und benötigt die Identitäten der Benutzer.
Identity Provider: Verwaltet die Identitäten der Benutzer und stellt sogenannte Assertions (Zusicherung) aus, welche die Identitäten der Benutzer bescheinigen.

6.11 Wie kann der Austausch von Sicherheitsinformationen klar definiert werden?

Durch die Verwendung von klar definierten Strukturen zum Austausch von Sicherheitsinformationen. Ein Beispiel ist das XML-basierte SAML welches sich unterteilt in Assertions (Authentifizierung, Autorisierung und weitere Session Attribute), Protocol (definiert wie Assertions angefordert und übermittelt werden) sowie die Bindings und Profile (definieren wie Assertions in Standard Transport- und Messaging-Framworks eingebunden werden).

6.12 Beschreiben Sie einen Authentifizuerngs-Assertion Aufbau.

Enthällt folgende Informationen:

- ID des Ausstellers und das Ausgabedatum
- Assertion-ID
- Subject (derjenige, der die Assertion zugeordnet wird)
- Bedingungen unter denen eine Assertion gültig ist
- Angaben, wie die Assertion erstellt wurde

6.13 Warum wird einie Assertion-ID benötigt.

Wenn ich mit verschiedenen Assertions vom selben Aussteller arbeite, muss ich die Assertions trotzdem unterschieden können.

6.14 Erklären Sie Role-based Access-Control.

Es handelt sich um eine aufgabenorientierte Rechtevergabe durch Rollen und Nachbildung von Organisationsstrukturen. Eine Rolle beschreibt eine Aufgabe bzw. die damit verbundenen Verantwortlichkeiten, Pflichten und Berechtigungen. Jeder Benutzer hat pro Sitzung eine aktive Rolle mit entsprechenden Zugriffsrechten.

6.15 Bewerten Sie Role-based Access-Control.

Erhöhung von Sicherheit und Qualität durch höhere Rechteaktualität, Nachvollziehbarkeit der Rechtevergabe und eine bessere Durchsetzbarkeit der technischen Sicherheitspolicies.
Vereinfachung der Rechteverwaltung durch eine Reduktion der Gesamtkosten und Bearbeitungszeiten/Freischaltzeiten, eine bessere Beherrschbarkeit sowie der Einführung eines Single-Point-of-Administration und Delegation der Rechteverwaltung.
Allerdings ist es als übergreifender Ansatz schwer umsetzbar, da die Komplexität der Modellierung hoch ist und die benötigten Werkzeuge komplex sind.

6.16 Erklären Sie das Zugriffsmatrix-Modell

Besteht aus einer veränderlichen Menge an Objekten und Subjekten. Des Weiteren gibt es eine Menge von Rechten (z.B. read, write, execute). Jede Datei/Prozess wird dann als eigene Spalte mit den entsprechenden Rechten abgebildet.

6.17 Nennen Sie Vor- und Nachteile vom Zugriffsmatrix-Modell

Vorteile:

- Sehr einfach und intuitive nutzbar
- Flexibel
- Einfach zu implementieren

Nachteile:

- Fehlende Typisierungskonzepte
- Keine Rechtevergabe an Klassen mit Rechte-Vererbung
- Skaliert schlecht durch eine hoch dynamische Menge an Subjekten

6.18 Nennen und erklären Sie weitere Pattern für Zugriffe.

- Bell-LaPadula-Modell: Systeme mit der Notwendigkeit, Informationsflüsse zu kontrollieren. Nur Subjekte mit einer Sicherheitsfreigabe (control Zugriffsrecht) darf auf ein Objekt zugreifen. Problem ist, dass Informationen/Objekte sukzessiv immer höher eingestuft werden. Daher kann man blind Schreiben, aber anschlieend nicht mehr lesen, da die Rechte nicht vorhanden sind.

- Chinese Wall Modell: Geeignet in Umgebungen, in denen Interessenkonflikte eine Rolle spielen können (z.B. Anwaltskanzlei). Objekte werden dafür in unterschiedliche Konfliktklassen eingeteilt und Zugriffe sind abhänig von der Zugriffshistorie, je nach vergangenen Zugriffen wird eine Zugriffsmauer aufgebaut.

6.19 Beschreiben Sie Access Control Requirements nach dem I&A Modell.

1. Festlegen der Domäne, in welcher Zugangskontrolle verwendet wird
2. Begrenzungen/besondere Eigenschaften erfassen (beeinflussen Anforderungen und deren Priorisierung)
3. Zugangskontrollregelwerk festlegen (z.B.: Closed System mit RBAC)
4. Granularitätslevel festlegen, auf dem Zugangskontrolle angewendet wird (Bsp Datenbank: Pro Datenbank, pro Tabelle, pro Zeile in Tabelle, pro Feld, ...)
5. Spezifische Anforderungen fur Domäne festlegen unter Verwendung der oben genannten allgemeinen Anforderungen
6. Wichtigkeit der Anforderungen festlegen (siehe Tabelle nächste Folie)

7 Fragen zu 05-Security Testing

TODO

8 Fragen zu 06-Sicherer Betrieb

TODO