Risicoanalyse/Beveiligingsanalyse

De risicoanalyse heeft tot doel per project zwakheden in de beveiliging of opzet van de software te vinden en te onderkennen. (Bron: Edhub, Grip op Secure Software, 4.3, alinea 1)

Het eindresultaat van de risicoanalyse is een lijst met dreigingen die relevant worden geacht voor de IT-middelen binnen de scope en inzicht in de ernst van deze dreigingen. (Bron: Edhub, Grip op Secure Software, 4.3, alinea 15)

Het doel van de risicoanalyse is het in een zo vroeg mogelijk stadium identificeren en begrijpen van risico's en het benoemen van mitigerende beveiligingseisen. (Bron: Edhub, Grip op Secure Software, 4.3, alinea 16) *(zo… lekker concreet op Edhub allemaal)

Inschatting van dreigingen via STRIDE

De analysemethode STRIDE is ontwikkeld door Microsoft. Dit is een 'threat assessment'. Er wordt een decompositie uitgevoerd, waarna per relevante component de gevoeligheid voor dreigingen wordt geanalyseerd. (Bron: Edhub, Grip op Secure Software, 4.3, alinea 9)

De naam STRIDE is een afkorting van de benamen van zes categorieën aan dreigingen, namelijk:

- Spoofing (misbruik van de gebruikersidentiteit, namelijk zich als een ander voordoen);
- Tampering (schending van de Integriteit);
- Repudiation (weerlegbaarheid);
- Information disclosure (schending van de privacy of het lekken van data);
- Denial of Service (DoS) (on-beschikbaarheid);
- Elevation of privilege (misbruik van bevoegdheden)

Op basis van deze dreigingen voer ik de risico/beveiligingsanalyse uit.

Kwalificering Risico's

De kwalitatieve risicoanalyse gaat uit van scenario's en situaties. Hierbij worden de kansen dat een dreiging werkelijkheid wordt ingeschat op basis van vuistregels en waarschijnlijkheid. De kwantitatieve risicoanalyse probeert op basis van risicowaardering te berekenen hoe groot de kans is dat een dreiging een incident wordt (Bron: pinkelephant.nl Risicoanalyse)

Risico (per dreiging)			
	Omvang van de schade door een dreiging		
Kans van optreden	**Laag**	**Midden**	**Hoog**
Laag	Laag	Laag	Midden
Midden	Laag	Midden	Hoog
Hoog	Midden	Hoog	Hoog

Afbeelding bron: (Edhub, Grip op Secure Software, 4.3

De lijst met dreigingen:

- Spoofing (misbruik van de gebruikersidentiteit, namelijk zich als een ander voordoen);
- Tampering (schending van de Integriteit);
- Repudiation (weerlegbaarheid);
- Information disclosure (schending van de privacy of het lekken van data);
- Denial of Service (DoS) (on-beschikbaarheid);
- Elevation of privilege (misbruik van bevoegdheden)

Over het algemeen worden de bovengenoemde dreigementen opgevangen door de Spring Security Framework (mits deze goed is toegepast m.u.v. Dos.). Dit besef is meegenomen in de kwalificering "kans van optreden". Toch kan het zomaar optreden dat een hacker een van de bovengenoemde dreigementen kan uitvoeren. Hoe groot is dan de impact op gebruikers of het bedrijf?
Hieronder volg de kwalificering voor kans van optreden en de impact bij optreden.

Impact →		Laag	Midden	Hoog
	Hoog	Tampering Information Disclosure Elevation of privilege		
	Midden		Denial of Service	
	Laag	Repudiation	Spoofing	

Kans van optreden →

<u>Einde Risico-analyse</u>