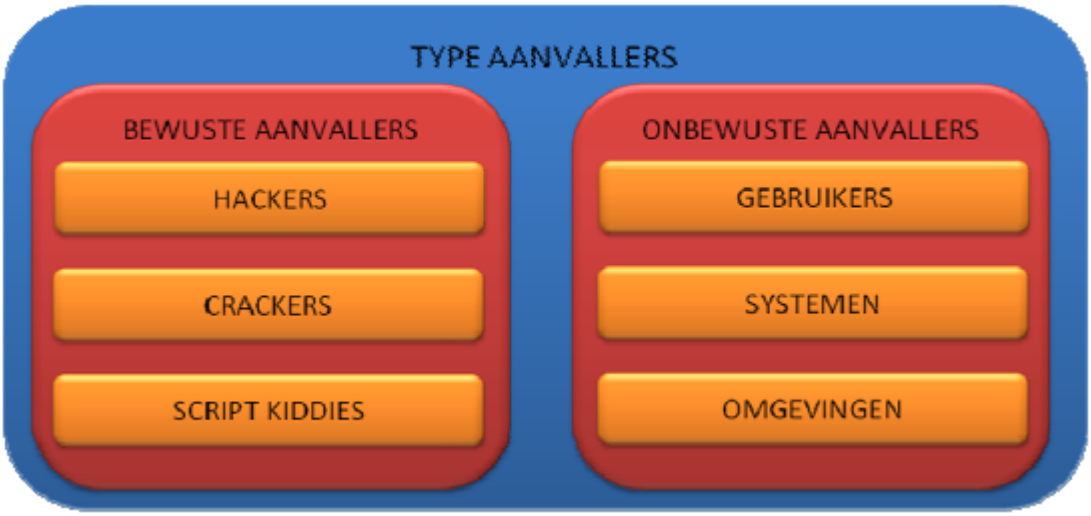

Belangrijke punten om te controleren:

- Het systeem is alleen te benaderen door personen met de juiste rechten. Dit voor zowel het officiële pad als ook via allerlei achterdeuren.
- Contact met andere applicaties moet veilig zijn. Indien er interactie is met andere systemen moeten alle inkomende berichten veilig zijn.
- Indien een gebruiker toegang heeft tot een applicatie door middel van tekstuele invoer moet deze invoer te allen tijde veilig zijn en mag deze niet leiden tot misbruik van de applicatie.
- Alle interactie die een gebruiker heeft met de applicatie moet gelogd zijn.
- Het moet niet mogelijk zijn ergens binnen de applicatie script/code uit te voeren.
- Het systeem mag door aanvallen van buitenaf nooit buiten werking zijn.
- Het is niet mogelijk dat klanten gegevens van anderen kunnen inzien of veranderen.
- Het is niet mogelijk de inlogfunctie te omzeilen.
- Het is niet mogelijk gegevens uit de database op te halen anders dan bedoeld.
- De gegevens die verzonden worden door de applicatie zijn versleuteld en niet gecodeerd.
- Het is niet mogelijk om via URL browsing andere functies aan te roepen dan gewenst.

- Foutmeldingen die getoond worden bevatten geen ongewenste informatie voor de eindgebruiker.

Punten telling voor technische beveiliging

Bij vertrouwelijkheid gaat het er om hoeveel data verloren kan gaan en hoe gevoelig deze data is:

- Minimale niet gevoelige data is “ontsnapt” (2 punten)
- Minimale gevoelige data is “ontsnapt” (6 punten)
- Maximale niet gevoelige data is “ontsnapt” (6 punten)
- Maximale gevoelige data is “ontsnapt” (9 punten)

Bij integriteit gaat het er om hoeveel data vernield kan worden. De mate waarin de gegevens een afspiegeling zijn van de werkelijkheid en niet gewijzigd kunnen worden:

- Minimale licht corrupte data (1 punt)
- Minimale zware corrupte data (3 punten)
- Maximale licht corrupte data (5 punten)
- Maximale zware corrupte data (9 punten)

De volgende stap is het in kaart brengen van het aantal systemen die mogelijk offline kunnen zijn door een aanval:

- Minimaal secundaire systemen zijn onderbroken (1 punt)
- Minimaal primaire systemen zijn onderbroken (5 punten)
- Veel secundaire systemen zijn onderbroken (5 punten)
- Veel primaire systemen zijn onderbroken (7 punten)
- Alle systemen zijn totaal onderbroken (9 punten)

Tenslotte gaat het er om of de aanvallers zijn aan te wijzen. Is het te achterhalen wie de aanval

heeft uitgevoerd?

- Volledig traceerbaar (1 punt)
- Mogelijk traceerbaar (7 punten)
- Volledig anoniem (9 punten)

Faalkans

Vaardigheden:

- Geen technische vaardigheden (1 punt)
- Enige technische vaardigheden (3 punten)
- Ervaren computergebruiker (4 punten)
- Netwerk en programmeer vaardigheden (6 punten)
- Beveiliging en penetration vaardigheden (9 punten)

Motivatie om het systeem te kraken:

- Laag of geen motief (1 punt)
- Mogelijke motief (4 punten)
- Hoog motief (9 punten)

De kwetsbaarheid van het systeem:

- Geen erkende toegang (0 punten)
- Beperkte toegang (4 punten)
- Volledige toegang (9 punten)

De omvang van de groep:

- Ontwikkelaars (2 punten)
- Beheerders (2 punten)
- Intranetgebruikers (4 punten)
- Partners (5 punten)
- Geautoriseerde gebruikers (6 punten)
- Anonieme internetgebruikers (9 punten)

Kans en schade klassen	
0 tot <3	LAAG
3 tot <6	MIDDEN
6 tot 9	HOOG

Risicoklasse per combinatie				
schade	Hoog	midden	hoog	kritisch
	Midden	laag	midden	hoog
	Laag	kennisgeving	laag	midden
		laag	midden	hoog
	faalkans			