Security-verslag

Inhoud

[Risicoanalyse 3](#_Toc531858631)

[DDOS-aanval 3](#_Toc531858632)

[Risico 3](#_Toc531858633)

[Analyse van waardevermindering 3](#_Toc531858634)

[Maatregelen 4](#_Toc531858635)

[Advies 4](#_Toc531858636)

[SQL-injecties 5](#_Toc531858637)

[Risico 5](#_Toc531858638)

[Analyse van waardevermindering 5](#_Toc531858639)

[Maatregelen 5](#_Toc531858640)

[Advies 6](#_Toc531858641)

[Ingebouwd veiligheidsniveau 7](#_Toc531858642)

[Vervolgstappen 8](#_Toc531858643)

# Risicoanalyse

## DDOS-aanval

### Risico

Een Distributed Denial of Service (DDoS) aanval is een aanval waarmee meerdere computers continu verbinding maken met één server of herhalend een handeling op de website uitvoeren. De gevolgen van een DDOS-aanval kan zijn dat de servers traag of zelfs onbereikbaar worden. Dit kan dan ook weer leiden tot reputatieverlies van WWI.

Een DDoS wordt opzettelijk opgezet door kwaadwillende mensen of door mensen die willen experimenten. Het opzetten van een DDoS-aanval is kinderspel, vanwege de hoeveelheid informatie die op internet te vinden is. Geef een amateur een paar uur, en diegene is ook nog eens ontraceerbaar.

Volgens een onderzoek van de Universiteit Twente zijn er dagelijks rond de 30.000 DDoS-aanvallen.

De kans dat een DDoS voorkomt is hierom relatief groot. De inschatting is dat WideWorldImporters zonder goede bescherming hier eens in de twee jaar mee te maken gaat hebben. Dit maakt de kans op een aanval 50% per jaar.

### Analyse van waardevermindering

De waarde die je kan verliezen door zo’n aanval is groot, er is hiervoor een inschatting gemaakt met wat er verloren kan gaan:

Stel dat WWI 15 bestellingen krijgt per dag en rond de 10 nieuwe mensen de webshop voor het eerst vinden. De 15 bestellingen hebben een gezamenlijke waarde van 800 euro.

Wanneer de website niet meer te bereiken zou zijn voor een tijd van 8 uur, betekent dit dat WWI een bedrag van 96.000,- euro mis zal lopen. Daarnaast loopt WWI 80 nieuwe klanten mis die de website niet kunnen bereiken. Hierdoor zakt de reputatie van WWI en komen er minder nieuwe mensen de webshop bezoeken.

De totaal ingeschatte waarde die WWI kwijt kan raken bij een DDoS-aanval ligt op 48.000,- euro per jaar (96000 \* 0,5).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dreiging | Schade | Kans | Maatregel | Rest-risico |
| DDoS aanval door het overbelasten van de website aan de hand van vele requests. | Medium | Medium | Een goede Internet service provider kiezen die zich goed kan beschermen tegen DDoS aanvallen | Laag |
| DDoS aanval door het overbelasten van de database door via formulieren te veel informatie te verzenden. | Medium | Medium | Captcha- gebruiken bij formulieren om een overbelasting van de servers te voorkomen. | Laag |

### Maatregelen

Door deze maatregelen toe te passen, zakt het risico aanzienlijk. Dit is omdat veel DDoS-aanvallen van een relatief simpele aard zijn. Veel amateurs worden door deze maatregelen geweerd; iets wat WWI voor veel schade behoed. Grootschalige, professionele aanvallen blijven een probleem voor WideWorldImporters. Dit is omdat hier niks tegen gedaan kan worden. Toch hoeft WWI niet actief te zoeken naar verdere maatregelen, omdat reguliere webshops maar weinig slachtoffer worden van grootschalige aanvallen.

### Advies

Het advies is om een goede, sterke internet service provider te kiezen die de website kan hosten. Het ontwikkelteam heeft Captcha geïntegreerd in de website, wat het voor robots onmogelijk maakt om grootschalig formulieren te verzenden naar de database. Captcha werkt aan de hand van een invul-vakje, wat alleen mensen kunnen aanvinken. Op deze manier worden mensen en robots van elkaar onderscheidden.

## SQL-injecties

Een belangrijk onderdeel van een website is de manier waarop het omgaat met zogeheten ‘SQL-injecties’. Op veel plekken in de webshop wordt de database opgeroepen omdat een gebruiker een actie wil ondernemen. Denk hierbij aan het weergeven van informatie van een specifiek artikel, of het bladeren en zoeken in artikelgroepen.

Als bij dit soort gevallen de input van een gebruiker benodigd is, dan ontstaat er een kwetsbaarheid. De gebruiker kan namelijk als input een stukje code meesturen, waardoor er allerlei mogelijkheden ontstaan om de database te ontregelen. Dit wordt in de ICT-wereld een ‘SQL-injectie’ genoemd.

### Risico

Omdat SQL-injecties relatief makkelijk zijn om in te voeren, moet hier zeker aan worden gedacht tijdens de ontwikkeling van de webshop. In het ergste geval kan iemand de database verwijderen. Door dit soort acties kan dus een enorme schade worden aangericht. Het is dus van belang dat de webshop tegen dit soort aanvallen wordt beschermt.

### Analyse van waardevermindering

De webshop zou in het slechtste geval bij een succesvolle SQL-injectie zijn database volledig kwijt raken. Alle artikelen, de voorraad, personen, facturen etc. moeten dan opnieuw worden ingevoerd. In het positiefste geval zal dit een maand in beslag nemen. Daarnaast zal WideWorldImporters enorme imagoschade leiden. De vraag blijft of de reputatie van deze ‘onveilige’ website ooit nog weer op te bouwen zou zijn na een datalek.

Uitgaande van 15 kopers en 10 nieuwe bezoekers per dag zal WWI 15(bezoekers) x 30(dagen) = 450 kopers mislopen met een totale financiële schade van: 800eu(Omzet per dag) x 30 (dagen) = €24.000,-. Dit zijn alleen de absolute getallen. Over de afname aan klanten en bezoekers valt alleen maar te speculeren. Het ontwikkelteam schat in dat het aantal kopers zal halveren, omdat zij geen zaken willen doen met een onbetrouwbare website.

Dit voorbeeld laat zien dat de schade van dergelijke SQL-injecties groot zal zijn, waarbij het realistisch is dat WideWorldImporters haar deuren zal moeten sluiten.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dreiging | Schade | Kans | Maatregel | Restrisico |
| Database verwijdert door SQL-injectie | Hoog | Hoog | Het indekken van de SQL-injectie aan de hand van een PDO-functie. | Laag |
| Toegang krijgen tot klantgegevens etc. door SQL-injectie | Hoog | Hoog | Het indekken van de SQL-injectie aan de hand van een PDO-functie | Laag |

### Maatregelen

Voor de verbinding tussen de database en de website wordt via PHP een medium gebruikt, genaamd PDO. PDO kan aan de hand van query’s iets oproepen uit de database en zet de uitkomst in een object. Met deze opgehaalde informatie kun je de website een actie laten uitvoeren. Na enig onderzoek naar de werking van PDO stuitte het ontwikkelteam op een functie binnen PDO, die automatisch beveiligt tegen SQL-injecties. Tests wijzen uit dat SQL-injecties niet meer mogelijk zijn als de database wordt opgeroepen met deze functie.

Het ontwikkelteam heeft besloten om deze functie direct toe te passen op de website om het risico te verkleinen.

### Advies

Het ontwikkelteam geeft als advies aan WideWorldImporters om de ontwikkelingen rond SQL-injecties nauwlettend in de gaten te houden. Veranderingen binnen PDO, PHP of SQL kunnen er toe leiden dat de beschermende functie niet meer werkt, en de website weer zeer kwetsbaar is voor SQL-injecties.

# Ingebouwd veiligheidsniveau

# Vervolgstappen