Security-verslag

Inhoudsopgave

[Risicoanalyse 3](#_Toc531868963)

[DDOS-aanval 3](#_Toc531868964)

[Risico 3](#_Toc531868965)

[Analyse van waardevermindering 3](#_Toc531868966)

[Maatregelen 4](#_Toc531868967)

[Advies 4](#_Toc531868968)

[SQL-injecties 5](#_Toc531868969)

[Risico 5](#_Toc531868970)

[Analyse van waardevermindering 5](#_Toc531868971)

[Maatregelen 5](#_Toc531868972)

[Advies 6](#_Toc531868973)

[Wachtwoordenlek 7](#_Toc531868974)

[Risico 7](#_Toc531868975)

[Algemene verordeningen gegevensbescherming 7](#_Toc531868976)

[Analyse van waardeverminden 7](#_Toc531868977)

[Maatregelen 7](#_Toc531868978)

[Advies 8](#_Toc531868979)

[Ingebouwd veiligheidsniveau 9](#_Toc531868980)

[Vervolgstappen 10](#_Toc531868981)

# 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.

## Wachtwoordlek

### Risico

Het risico bij webshops met een inlogfunctie is dat de wachtwoorden die worden opgeslagen kunnen uitlekken. De meeste klanten gebruiken één wachtwoord voor meerdere accounts waardoor kwaadwillenden op meerdere websites kunnen inloggen van de getroffen klant.

Gemiddeld zit iemand met zijn gegevens in honderden tot duizenden bestanden, zowel van het bedrijfsleven als van de overheid. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens voldoende worden beveiligd. Slechte beveiliging kan leiden tot een datalek en vervolgens tot misbruik van deze gegevens. Bijvoorbeeld voor identiteitsfraude.

### Algemene verordeningen gegevensbescherming

Bedrijven en overheden die persoonsgegevens gebruiken moeten deze volgens de Algemene verordening gegevensbescherming (AVG) beveiligen. Zo voorkomen ze datalekken.

Volgens de AVG moeten bedrijven en overheden hiervoor passende technische en organisatorische maatregelen nemen:

* Organisaties moeten moderne techniek gebruiken om persoonsgegevens te beveiligen.
* Verder moeten ze niet alleen naar de techniek kijken, maar ook naar hoe ze als organisatie met persoonsgegevens omgaan. Wie heeft er bijvoorbeeld toegang tot welke gegevens?
* Organisaties die persoonsgegevens gaan verzamelen, moeten vooraf nadenken over de beveiliging hiervan. En beveiliging van persoonsgegevens moet binnen een organisatie een blijvend punt van aandacht zijn.
* Als organisaties andere partijen inschakelen om persoonsgegevens te verwerken, dan moeten deze verwerkers voldoende maatregelen treffen om de gegevens te beveiligen. Organisaties die gegevensverwerking door een verwerker laten uitvoeren, blijven verantwoordelijk voor de naleving van de AVG.

### Analyse van waardeverminden

Als dit een bedrijf treft, ontstaat er een groot probleem, klanten verliezen hun vertrouwen in het bedrijf. Zij zouden dus niet snel iets meer kopen, dit zorgt voor verlies in zowel geld als in klanten.

Stel dat het bedrijf per dag 15 bestellingen met een totale omzet van 800euro heeft en 10 nieuwe mensen die de webshop voor het eerst bezoeken. Het onderzoeksteam is tot de conclusie gekomen dat de bestellingen omlaag zullen gaan. Hierdoor daalt de omzet. Het onderzoeksteam schat dat de bestellingen met 33% zullen dalen. Dit houd in dat er maar 10 bestellingen worden geplaatst per dag met een omzet van 530 euro, dat houd in dat het bedrijf 8000 euro per maand misloopt. Hier zal het bedrijf ontzettend veel last van krijgen. Naast deze financiële schade zal WideWorldImporters veel reputatieschade lijden, wat hoogstwaarschijnlijk voor nog minder omzet zal zorgen.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dreiging | Schade | Kans | Maatregel | Rest-risico |
| Wachtwoorden lekken uit via een datalek. | Hoog | Medium | Wachtwoorden die worden opgeslagen worden gehashed in en beveiligde database. | Laag |

### Maatregelen

De maatregelen die hier tegen kunnen worden genomen is als eerste de database beveiligen met een goed wachtwoord. Het wachtwoord is op dit moment leeg en moet dus aangepast worden naar een lang en sterk wachtwoord. Met sterk wordt bedoeld dat het wachtwoord uit een minimum aantal tekens moet voldoen, een speciaal teken, een cijfer en een hoofdletter bevat.

Stel dat er iemand is die dit wachtwoord doorbreekt dan is het goed dat de wachtwoorden zijn gehashed. Een hash-waarde (of hashes) is het best te vergelijken met een digitale vingerafdruk. Het identificeert iedere tekstreeks of bestand via een reeks getallen. Als twee bestanden of tekenreeksen dezelfde hash-waarde hebben dan kun je er (bijna) zeker van zijn dat ze identiek zijn. Als degene de wachtwoorden wil zien moet het een hash hebben om het wachtwoord te laten zien. De kans dat een hash geraden word is minimaal. Het ontwikkelteam heeft deze maatregel toegepast op de database.

### Advies

Het advies van het ontwikkelteam is als volgt: Verander het wachtwoord van de database (omdat het ontwikkelteam het huidige wachtwoord weet) en doe dit regelmatig. Zorg ervoor dat alleen de medewerkers die dit wachtwoord echt nodig hebben weten.

## SSL-certificaat

Op dit moment draait alles nog op localhost, nadat de website goedgekeurd is en online gezet wordt moet er een SSL-certificaat geïmplementeerd worden. Een SSL certificaat is een bestand dat zorgt voor een betere beveiliging van gegevens tussen de server (van jouw website) en een internet browser (zoals Chrome of Internet Explorer). SSL staat letterlijk voor Secure Sockets Layer wat betekent dat er een beveiligde laag geplaatst wordt tussen een server en een internet browser waardoor de gegevens beveiligd worden.



Als je het SSL-certificaat hebt ingevoerd dan krijg je een slotje en https op je website, klanten zullen dit zien en vertrouwen de site dan beter. Zij durven hier makkelijker hun betaalgegevens in te voeren dan op een niet beveiligde site, dit zorgt dus voor meer orders.

# Ingebouwd veiligheidsniveau

# Vervolgstappen