Door: Julian, Jochem, Ruben, Wytze en Melvin

Datum: 4-12-2019

Klas: ICTM1C

Groep: 5

Verslag Security (concept)

Inhoudsopgave

[**1.** **Inleiding** 2](#_Toc27405766)

[**2.** **Risicoanalyse** 3](#_Toc27405767)

[2.1 Server Crash 0](#_Toc27405768)

[2.2 Dreiging: DDoS-aanval 0](#_Toc27405769)

[2.3 Dreiging: Data corruptie 0](#_Toc27405770)

[2.4 Dreiging: Ransomware 0](#_Toc27405771)

[2.5 Dreiging: Security bij het hostingbedrijf 1](#_Toc27405772)

[2.6 Dreiging: Phishing e-mails 1](#_Toc27405773)

[2.7 Dreiging: SQL-Injecties 2](#_Toc27405774)

[2.8 Dreiging: Cross-site scripting 2](#_Toc27405775)

[2.9 Datalek 2](#_Toc27405776)

[**3.** **Beschrijving ingebouwd veiligheidsniveau** 4](#_Toc27405777)

[3.1 SQL-injecties 4](#_Toc27405778)

[3.2 Cross-site scripting 4](#_Toc27405779)

[3.3 Datalek 4](#_Toc27405780)

[**4.** **Advies over vervolgstappen** 5](#_Toc27405781)

[4.1 Ransomware 5](#_Toc27405782)

[4.2 Phishing e-mails 5](#_Toc27405783)

[**5.** **Bronvermelding** 6](#_Toc27405784)

*Paginanummer en opmaak hebben we nog niet correct in het concept verslag.*

# **Inleiding**

In dit verslag wordt een risicoanalyse beschreven met betrekking tot de webshop van het bedrijf Wide World Importers (WWI). WWI heeft een belang bij een nieuwe webshop om de verkoop te starten in Europa. Wij hebben een risicoanalyse uitgevoerd met de betrekking tot de veiligheid. We hebben dit uitgevoerd op basis van de ervaring in de praktijk en door middel van onderzoek naar internetveiligheid. Alle beveiligingspunten zijn benoemd in dit verslag met eventuele uitleg en de prioriteit van deze beveiligingspunten. Het doel van dit verslag is om WWI te adviseren over de veiligheid van hun nieuwe webshop.

# **Risicoanalyse**

*Tabel 1: risicoanalyse*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Nr** | **Dreiging** | **Schade** | **Kans** | **Maatregel** | **Restrisico** | **Beveiligingsaspect** |
| 2.1 | Server crash | H | M | De servers laten regelen door een hostingbedrijf. | M | Beschikbaarheid |
| 2.2 | DDoS-aanval | H | H | Betere beveiliging tegen pakketten die binnenkomen en naar buiten gaan. | M | Beschikbaarheid |
| 2.3 | Data corruptie | H | M | Back-ups maken | L | Beschikbaarheid, Integriteit en Vertrouwelijkheid |
| 2.4 | Ransomware | H | H | Personeel bewust maken | M | Beschikbaarheid en Vertrouwelijkheid |
| 2.5 | Security bij het hostingbedrijf | M | L | Maak gebruik van HTTPS en SSL en check of alle beveiligingsmaatregelen in het bedrijf op orde zijn. | L | Beschikbaarheid en Vertrouwelijkheid |
| 2.6 | Phishing e-mails | H | H | Informeer medewerker over hoe ze het beste tegen phishing in kunnen gaan zodat er geen schade ontstaat. | M | Vertrouwelijkheid |
| 2.7 | SQL-Injecties | H | H | Gebruik prepared statements voor opdrachten in de database. | L | Beschikbaarheid, vertrouwelijkheid en integriteit |
| 2.8 | Cross-site scripting | M | M | Zorg ervoor dat gebruikers altijd correct doorverwezen worden naar beveiligde pagina’s. | L | Vertrouwelijkheid |
| 2.9 | Datalek | H | M | Zorg dat de gegevens alleen door de personen die ze nodig hebben bekeken en eventueel bewerkt kunnen worden. | L | Vertrouwelijkheid |

## 2.1 Server Crash

Als de server crasht hebben klanten en personeel geen toegang meer tot de website. De server kan crashen door menselijke of door niet-menselijke oorzaken. Aan menselijke oorzaken kan vaak wat worden gedaan, maar aan niet-menselijke oorzaken kan niet altijd iets aan gedaan worden. Een voorbeeld van een menselijke oorzaak is een hacker die toegang weet te krijgen tot de server. De hacker kan dan de server platleggen. Enkele voorbeelden van niet menselijke oorzaken: brand in de serverkamer van WWI of door slechte weersomstandigheden de stroom uitvalt of wateroverlast.

Het risico hiervan is dat de webshop niet online staat en de verkoop van producten stil komt te liggen. Dit probleem moet opgelost worden. De impact hangt af van hoelang dit duurt: Als de webshop er 10 minuten uitligt zal het financieel minder schade aanrichten, maar als de webshop er 24 uur uitligt is dat een flinke financiële klap. Doordat de webshop niet meer online staat, tonen bezoekers meer interesse in de concurrent en hiermee verliest WWI ook (potentiële) klanten.

Een oplossing zou zijn om de server op twee locaties, oftewel bij twee aparte hostingbedrijven te laten draaien. Dit verhelpt het probleem als één van de twee bedrijven problemen krijgt d.m.v. stroomuitval, wateroverlast of een crash. Hierdoor kan de website verder draaien bij het andere hostingbedrijf. Natuurlijk kan het voorkomen dat beiden servers problemen krijgen, hierdoor zou je een derde server kunnen laten draaien, maar financieel gezien is dat niet de beste oplossing.

## 2.2 Dreiging: DDoS-aanval

DDoS staat voor Distributed Denial of Service. Met een DDoS-aanval maken een grote hoeveelheid computers, vaak vanaf verschillende locaties ter wereld, tegelijkertijd verbinding met één server. De mensen achter de aanval proberen deze server traag te maken, en hun uiteindelijke doel is om de server onbereikbaar te maken. Een DDoS-aanval wordt veroorzaakt door een server te overspoelen met webverkeer. De server krijgt op zo’n moment meer data binnen dan hij kan verwerken, waardoor het onbereikbaar wordt.

Om dit voor elkaar te krijgen, worden vaak botnets ingezet. Botnets zijn verzameling van softwarerobots, die automatisch en zelfstandig bezig kunnen. Het is voor hackers dus erg voordelig om bots te gebruiken, omdat ze niet alleen weinig werk hebben aan de aanval maar vooral omdat het een erg goedkope manier is om een server onbereikbaar te maken. Onbereikbaarheid van de server kan voor de webshop veel geld kosten, zeker als de server er langer dan een paar minuten er uit ligt. Daarom is een optimale veiligheid zo belangrijk om de webshop te beschermen.

(KPN, 2018)

Volgens Realhosting.nl (2019) is een botnet een groot netwerk van computers welke besmet zijn met bijvoorbeeld malware. Sommige botnets bevatten wel miljoenen besmette computers. Als de hacker genoeg computers heeft besmet, kan hij vanuit een centraal punt de computers aansturen om een bepaalde opdracht uit te voeren. De computers kunnen bijvoorbeeld de webshop continu bezoeken, wat de server niet aankan. Een normale bezoeker kan vervolgens niet bij de webshop, en als deze aanval een tijdje duurt heeft dat grote gevolgen voor de inkomsten van WWI.

## 2.3 Dreiging: Data corruptie

Tegenwoordig is data een van de belangrijkste bezitten voor een bedrijf. Deze data wordt opgeslagen op servers en databases. Als data corrupt raakt, kan dat voor (enorm veel) verlies zorgen. Als data corrupt raakt betekent dit dat de data niet meer toegankelijk is en als verloren kan worden beschouwd.

Een maatregel die bedrijven kunnen nemen om dit te voorkomen is regelmatig back-ups te maken van data en systemen. Als er dan corrupte data ontstaan, is het mogelijk om dit terug te zetten middels een eerder gemaakte back-up. Het nadeel hiervan is dat de data tussen de vorige back-up en nu verloren gaat. Een andere optie is data recovery. Bedrijven kunnen data recovery experts inhuren om te kijken of corrupte data nog te repareren valt.

De impact van data corruptie is hoog want als er belangrijke gegevens corrupt worden is de kans heel groot dat het bedrijf deze gegevens niet meer terug kan halen. Dit kan het bedrijf veel geld kosten.

De kans dat dit gebeurd is wel laag wat meestal zijn het kleine fouten die dit probleem veroorzaken.

## 2.4 Dreiging: Ransomware

Bestanden op computers kunnen worden besmet door bijvoorbeeld een bijlage in een e-mail te openen of tijdens het surfen op het internet. Ransomware wordt ook verstopt in advertenties. Klikken op de advertenties is soms nieteens nodig om besmet te raken. Het openen van een pagina is soms al voldoende.

Bedrijven, vooral midden-en kleinbedrijven, worden veel per mail benaderd. De ransomware wordt geïnstalleerd als een bijlage in een e-mail wordt geopend. Ook raken bedrijven vaak besmet doordat werknemers hun privémail bekijken op bedrijfscomputers.

Soms gaat besmetting via de computer gepaard met telefooncontact. Een slachtoffer wordt dan eerst telefonisch verleid om naar een bepaalde pagina te surfen waar de besmetting plaatsvindt.

De ontwikkeling van ransomware gaat razendsnel. Met als gevolg dus ook de kans en mogelijkheden om besmet te raken. Bovenstaande risico’s zijn dan ook slechts een indicatie.

(Politie.nl, z.d.)

Als een van de medewerkers van WWI per ongeluk ransomware op zijn of haar werkcomputer installeert kan het gevolg heel groot zijn. Ransomware zorgt dat bepaalde data en bestanden vast worden gezet. Het komt er dan op neer dat er een slot op deze data en bestanden wordt gezet. De enige manier om dit slot eraf te halen is meestal een heel groot bedrag betalen (ransom) aan de partij, meestal hackers, die de ransomware software heeft ontwikkeld.

Gevolgen voor het bedrijf zijn dat alles plat ligt en dat er geen producten verkocht kunnen worden. Dit resulteert in verlies voor WWI. Ook ligt alle data in handen van de groep die de ransomware heeft ontwikkeld, dit kan het bedrijf erg veel geld kosten. Tegenwoordig is het risico van ransomware op een computer binnen een bedrijf heel groot.

Een besmetting van ransomware op een computer heeft altijd een menselijke oorzaak. Soms wordt er een usb in een werk computer gedrukt waar ransomware op staat zonder dat iemand daar iets van weet en soms wordt er op een verkeerd linkje geklikt in een e-mail. Om dit te voorkomen is het belangrijk dat het personeel goed is ingelicht over de gevaren van ransomware en hoe het in zijn werk gaat.

De impact van deze dreiging is hoog omdat er veel data verloren kan gaan in het geval er niet betaald wordt.

## 2.5 Dreiging: Security bij het hostingbedrijf

Als er securityproblemen zijn met het hosting bedrijf die de webshop draait, is dit (afhankelijk van hoelang het probleem bestaat) een probleem voor WWI. Een hacker kan mooi gebruik maken van de problemen door bijvoorbeeld de webshop offline te halen. Hierdoor kunnen er geen producten gekocht worden, waardoor WWI geen inkomsten heeft.

Ook is het een noodzaak om te checken hoe het hostingbedrijf de security voor elkaar heeft. Hoe zijn de poorten geconfigureerd? Is het mogelijk voor hackers om binnen te komen? Maakt het hostingbedrijf gebruik van HTTP of HTTPS? Gebruiken ze SSL? Als deze zaken slecht geregeld zijn, zal de impact van een hacker groot zijn.

Er kunnen veel verschillende oorzaken zijn voor securityproblemen binnen het hostingbedrijf, dus is het moeilijk te zeggen wat voor verschillende maatregelen er genomen kunnen worden om dit op te lossen. Om te zorgen dat de security in de browser in ieder geval in orde te maken is het noodzakelijk om HTTPS en SSL te gebruiken.

De kans dat dit soort problemen voorkomen is klein, omdat hosting bedrijven vaak gespecialiseerd zijn in dit soort services en meestal binnen minuten/uren het probleem gerepareerd hebben.

## 2.6 Dreiging: Phishing e-mails

Phishing is het verkrijgen van persoonlijke informatie doormiddel van bijvoorbeeld een nep e-mail van een bank of een instantie. Phishing komt heel veel voor via de mail. Oplichters sturen mensen een e-mail die bijna hetzelfde eruit ziet als een echte e-mail van de bank. Daarin wordt meestal gevraagd of het slachtoffer (de ontvanger van de phishing mail) even wil inloggen met hun bankgegevens. Oplichters hebben dan vaak een neppe site gemaakt die heel erg op de site van een bank lijkt om zo de bankgegevens van het slachtoffer te verkrijgen.

Een andere vorm van phishing kan zijn dat je bijvoorbeeld gebeld wordt dat er iets mis is met je computer. De oplichters zullen via een programma als teamviewer je computer overnemen en zo persoonlijke gegevens voor je neus weghalen. De impact kan dus hoog zijn, vooral als het om bedrijfsgegevens gaat.

Er wordt tegenwoordig veel aandacht aan besteed, op zowel tv als op het internet, om phishing tegen te gaan. Ook hoor je vaak dat instanties zoals banken en andere overheidsinstanties nooit persoonlijke gegevens vragen via e-mail. Phishing is eigenlijk een vorm van social hacking en kan worden tegengehouden door altijd alert te blijven op nep e-mails en telefoontjes.

## 2.7 Dreiging: SQL-Injecties

Bij een SQL-injectie kan een gebruiker toegang krijgen tot de gegevens uit de database door gebruik te maken van SQL-statements. Dit houdt in dat waar een gebruiker een zoekopdracht doet in de zoekbalk van de website uitvoert naar bijvoorbeeld een product, daar zou een hacker een sql query in kunnen stoppen die bijvoorbeeld alle gebruikers verwijdert uit een database.

Het risico hiervan is dat een hacker heel veel mogelijke aanpassingen kan doen in een database als dit niet goed beveiligd is.

Maatregelen wat hiertegen genomen kan worden is in de PHP-code alle SQL queries te beveiligen met iets wat prepared statements heet. Hierdoor wordt alleen de in de webshop geprogrammeerde query uitgevoerd en wordt de opdracht afgebroken op het moment dat er een andere opdracht in de SQL in voorkomt.

De kans dat dit tegenwoordig gebeurd is er hoog. Veel webshops zijn hier niet tegen beveiligd en kunnen daardoor klantgegevens kwijtraken.

Bij een SQL-injectie kan de gebruiker toegang krijgen tot gegevens (en wijzigen) uit de database door gebruik te maken van SQL-queries bij invoervelden van de website. Als de gebruikers toevllig

## 2.8 Dreiging: Cross-site scripting

Cross site scripting is de naam van een fout in de beveiliging van een webapplicatie. Het wordt veroorzaakt doordat de invoer die de webapplicatie ontvangt niet juist wordt verwerkt en hierdoor in de uitvoer terecht komt naar de eindgebruiker. Via deze fout in de security van een webapplicatie kan kwaadaardige code geïnjecteerd worden.[[1]](#endnote-2)

Hackers kunnen gebruikers door linken naar andere webpagina’s. Dit wordt meestal ook gebruikt in combinatie met phishing. Een gebruiker kan dan worden doorgestuurd naar bijvoorbeeld een site van een bank die precies uitziet als de echte site, terwijl de gebruiker eerst wel op de echte site van de bank zat.

De impact hiervan is hoog omdat het kan leiden tot klantgegevens verlies en dat kan heel veel geld kosten voor WWI.

## 2.9 Datalek

Gegevenslekken komen niet vaak voor maar hebben wel altijd een grote impact op het bedrijf. Het is het lekken van de gegevens buiten het systeem. Dit kan ernstige gevolgen hebben voor het bedrijf als het gevoelige informatie is die gelekt wordt.

In de meeste gevallen worden datalekken veroorzaakt door menselijke factoren. Dit kan zijn door een usb-stick die verloren wordt of doordat er iemand zonder de juiste rechten bestanden heeft bewerkt. Ook kan het zijn dat een hacker de bestanden heeft verkregen door in te breken in het systeem in welk geval de gestolen informatie voor veel problemen kan zorgen.

Gegevenslekken behoren tot een aanval op de vertrouwelijkheid en soms de integriteit van de informatie. In het geval dat de informatie alleen verloren of gedeeld wordt is het een aanval op de vertrouwelijkheid. Als de gegevens door iemand worden aangepast die hier geen toestemming voor heeft dan is het een aanval op de integriteit van de gegevens.

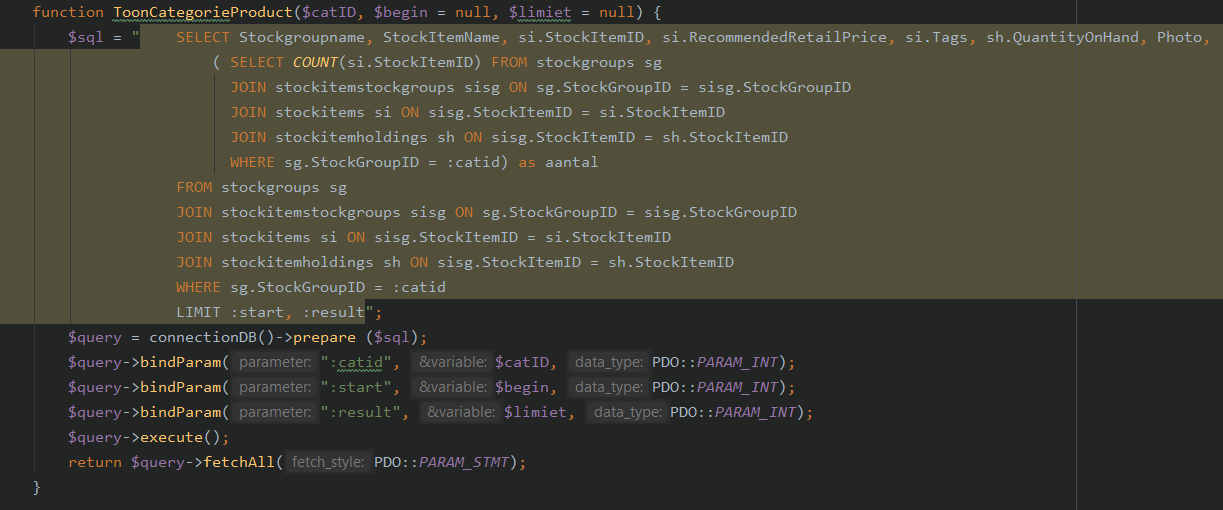
Er zijn verschillende manieren om datalekken te voorkomen. Als het datalek is veroorzaakt door een medewerker die een usb-stick is verloren is het verstandig om alleen de medewerkers met autoriteit over de informatie die er op de sticks staat met deze sticks overweg te laten gaan. Ook is het verstandig om de gegevens op de usb-stick te encrypten zodat als deze verloren wordt, de gegevens niet leesbaar zijn voor de vinder.

Als het datalek is veroorzaakt door een hacker die in het systeem is ingebroken moet er worden gekeken naar de manier waarop de hacker in het systeem gekomen is en moet ervoor worden gezorgd dat dit in de toekomst niet meer mogelijk is.

# **Beschrijving ingebouwd veiligheidsniveau**

## 3.1 SQL-injecties

In de code van de webshop hebben wij een aantal maatregelen geïmplementeerd om SQL-injecties te voorkomen. Een voorbeeld hiervan is dat wij de query helemaal ‘schoon’ maken voordat hij wordt uitgevoerd. Hieronder is de code te zien die wij gebruiken in een functie. De vijf regels code onder het gele gemarkeerde stuk (de query) zijn voor de beveiliging hiervan.



## 3.2 Cross-site scripting

XSS is te voorkomen door de input die van de gebruiker wordt verkregen te filteren voordat deze verwerkt wordt. Hierdoor kun je voorkomen dat er bijvoorbeeld code terechtkomt op plekken waar deze niet is toegestaan en zorg je ervoor dat de site naar behoren blijft functioneren.

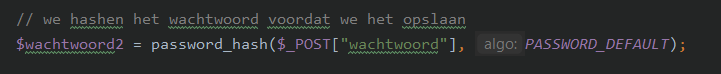
Ook kun je ervoor zorgen dat de output wordt gecontroleerd als deze te maken heeft met eerdere input van de gebruiker.

De oplossing die wij hebben gebruikt is $\_POST in plaats van $\_GET. Dit zorgt ervoor dat de gegevens die ingevoerd zijn niet zichtbaar zijn voor de gebruiker. In de url van de webshop worden alleen de nodige gegevens weergegeven.

## 3.3 Datalek

Een datalek is te voorkomen door ervoor te zorgen dat de informatie van je bedrijf veilig wordt opgeslagen. Er zijn veel verschillende methodes om dit te doen.

Wij hebben ervoor gekozen om onder andere het wachtwoord dat door de gebruiker wordt ingevuld te hashen (een willekeurige waarde in een vaste waarde veranderen). Dit doen we om te zorgen dat als de database gehackt wordt, de hacker de wachtwoorden niet kan lezen of gebruiken.



# **Advies over vervolgstappen**

Wij hebben al een aantal maatregelen genomen voor het beveiligen van de website, maar er blijven een paar risico’s liggen waar wij geen invloed over hebben. Over de volgende punten hebben wij geen invloed, maar er moet door WWI actie tegen ondernomen worden:

1. Ransomware
2. Phishing e-mails

## 4.1 Ransomware

Het is erg belangrijk om de medewerkers te informeren over ransomware. Bestanden op computers kunnen worden besmet door bijvoorbeeld een bijlage in een e-mail te openen of tijdens het surfen op het internet. Ransomware wordt ook verstopt in advertenties. Klikken op de advertenties is soms niet eens nodig om besmet te raken.

Het openen van een pagina is soms al voldoende. Hierdoor bestaat er altijd een risico dat een computer besmet geraakt kan worden, en vanaf dat punt zouden alle computers bij WWI besmet kunnen worden wat tot een lange downtime en veel losgeld leidt. Het is van belang dat iedere werknemer weet wat ransomware is en hoe zij er mee om kunnen gaan. Volgens veiliginternetten.nl (z.d.) zijn er een aantal punten waar je op moet letten bij ransomware:

1. Installeer updates van besturingssystemen en updates van programma’s direct. Dit is niet alleen goed voor de beveiliging, maar het zal ook goed zijn voor de snelheid en het aantal functionaliteiten van deze programma’s.
2. Gebruik antivirussoftware. Deze kan ransomware detecteren en blokkeren.
3. Open geen e-mails, links in e-mails en zeker geen bijlage(n) van onbekende afzenders. Open ook geen e-mails die u niet verwacht maar waar de afzender wel bekend is. Zie voor meer informatie kopje 4.2 Phishing e-mails.
4. Maak regelmatig backups, dit zorgt ervoor dat je niet alles kwijtraakt.

## 4.2 Phishing e-mails

Het is handig voor het ontwikkelteam om ervoor te zorgen dat de medewerkers zijn geïnformeerd over phishing e-mails. Dit is meer voor de veiligheid van de medewerkers zelf zodat hun persoonlijke gegevens veiliger zijn. Het is belangrijk dat medewerkers goed opletten als ze een mail binnenkrijgen van bijvoorbeeld een bank of een ander instantie. Er moet bijvoorbeeld worden gelet op wie de afzender is, en of dit niet een nep afzender is. Ook moet er gelet worden op de opmaak van het bericht, dat het niet erg nagemaakt lijkt. Als de mail niet verwacht wordt maar wel van de juiste afzender lijkt, kan het ook mis zijn. Medewerkers moeten worden gewaarschuwd om nooit hun gegevens in te voeren, en zeker niet de inloggegevens van hun functie bij WWI. Dit kan tot schade bij het bedrijf lijden.

# **Bronvermelding**

compromise.nl. (2019, 3 oktober). *Wat is een datalek? Melden of niet? Wat zijn de sancties?* Geraadpleegd op 16 december 2019, van <https://www.compromise.nl/blog/datalek-2/>

KPN. (2018, 5 juni). *Een DDoS attack: wat is het en wat zijn de gevolgen?* Geraadpleegd op 16 december 2019, van [https://www.internedservices.nl/blog/DDoS-attack-wat-is-gevolgen/](https://www.internedservices.nl/blog/ddos-attack-wat-is-gevolgen/)

Politie.nl. (z.d.). *Ransomware*. Geraadpleegd op 16 december 2019, van <https://www.politie.nl/themas/ransomware.html>

Realhosting.nl. (2019, 17 mei). *Wat is een DDoS aanval? - RealHosting.nl*. Geraadpleegd op 16 december 2019, van <https://realhosting.nl/helpdesk/wat-is-een-ddos-aanval/>

veiliginternetten.nl. (z.d.). *Hoe voorkom ik ransomware?* Geraadpleegd op 16 december 2019, van <https://veiliginternetten.nl/themes/situatie/hoe-voorkom-ik-ransomware/>

1. Wikipedia <https://nl.wikipedia.org/wiki/Cross-site_scripting> [↑](#endnote-ref-2)