Is je website veilig?

VERTROUWELIJK

Beveiligingstest door een Nederlandse ethisch hacker

Pentest-rapport

www.[jouwbedrijf].nl

Voorbeeldrapport: het bedrijf en de bevindingen zijn verzonnen

Bedrijf	Getest op	Getest door	Rapport
[Jouw bedrijf]	**[datum] en [datum]**	**[naam], Gomanche**	**Versie 1.0**

1 In één oogopslag

Eén ernstig lek moet vandaag dicht: een oude back-up met klantgegevens staat openbaar online. De andere punten kun je deze maand laten oplossen.

Daarna staat je website er goed voor: de basis, zoals het slotje en de WordPress-versie, is in orde.

RISICONIVEAU

Hoog

Laag · Middel · Hoog

Wat we vonden

1 Hoog risico · **3** Middel · **1** Laag · **4** In orde

Hoe erg is het?

Hoog risico

Iemand kan nu al bij je gegevens of je website. Laat dit vandaag of deze week oplossen.

Middel

Een aanvaller heeft er iets aan, maar heeft meer nodig. Laat dit deze maand oplossen.

Laag

Een kleine verbetering. Neem het mee bij het volgende onderhoud.

Wat we hebben gedaan

Op [datum] en [datum] heeft een ethisch hacker geprobeerd om binnen te komen op je website, zoals een crimineel dat zou doen. Dat gebeurde met je schriftelijke toestemming. We hebben niets veranderd of verwijderd, en geen gegevens bewaard.

- Je website, ook de pagina's achter het inlogscherm
- Je contact- en offerteformulier
- De plug-ins en het thema van je website
- De server waarop je website draait
- Je e-mailinstellingen

Wat goed gaat

- ✓ Je website heeft een beveiligde verbinding (het slotje), en stuurt iedereen daarheen.
- ✓ WordPress zelf is bijgewerkt naar de nieuwste versie.
- ✓ Je formulieren laten zich niet misbruiken om code in je website te zetten.
- ✓ Er zijn maar twee beheerders, allebei met een sterk wachtwoord.

Goed om te weten. Een pentest is een momentopname: een nieuwe update of een nieuw lek kan morgen een nieuw gat maken. Laat je website daarom elk jaar opnieuw testen, en na grote veranderingen. Dit rapport is vertrouwelijk; deel het alleen met wie het nodig heeft, zoals je webbouwer of je verzekeraar.

2 Wat we vonden

Per punt lees je wat er aan de hand is, wat er kan gebeuren en wat je moet doen. De technische details staan apart, voor je webbouwer.

HOOG RISICO

1 Een oude back-up met klantgegevens staat openbaar online

Wanneer
vandaag

Wat er aan de hand is

Op je website staat een back-up van vorig jaar. Iedereen die het adres van het bestand raadt, kan het downloaden. Er staan namen, e-mailadressen en telefoonnummers van ongeveer 1.200 klanten in.

Wat kan er gebeuren?

Criminelen zoeken automatisch naar zulke bestanden. Met je klantgegevens kunnen ze nepmail sturen die er echt uitziet. Heeft iemand het bestand al gedownload, dan is dat een datalek. Dat moet je binnen 72 uur melden bij de Autoriteit Persoonsgegevens.

Wat moet je do(e)n?

Laat je webbouwer het bestand vandaag verwijderen. Laat ook nagaan of het eerder is gedownload.

Wie: **je webbouwer**

</> VOOR JE WEBBOUWER

```
GET https://www.[jouwbedrijf].nl/backup-2025.zip → HTTP 200, 48 MB, bevat een databasedump (wp_users, wp_wpforms_entries).
Verwijder het bestand, controleer de toegangslogs op eerdere downloads en blokkeer .zip, .sql en .bak in de webroot.
```

MIDDEL

2 Een verouderde plug-in heeft een bekend lek

Wanneer
deze maand

Wat er aan de hand is

Je contactformulier werkt met een plug-in die al een jaar niet is bijgewerkt. In die versie zit een lek dat al maanden bekend is.

Wat kan er gebeuren?

Via dit lek kan een aanvaller je formulier misbruiken om spam te versturen, met jouw website als afzender. Je website kan daardoor op een zwarte lijst komen. Dan komt ook je eigen mail slechter aan.

Wat moet je do(e)n?

Laat je webbouwer de plug-in bijwerken. Spreek ook af wie voortaan elke maand de updates doet.

Wie: **je webbouwer**

</> VOOR JE WEBBOUWER

```
Plug-in [contactformulier] 5.2.1: bekend lek, opgelost in 5.3.0.
wp plugin update --all, en zet automatische updates aan voor plug-ins met beveiligingsfixes.
```

MIDDEL

3 Op je inlogscherm kun je eindeloos wachtwoorden proberen

Wanneer **deze maand**

Wat er aan de hand is

Op het inlogscherm van je website kun je zo vaak een wachtwoord proberen als je wilt. Wij probeerden er 500, zonder dat er iets gebeurde.

Wat kan er gebeuren?

Een aanvaller kan zo een zwak of eerder gelekt wachtwoord raden. Daarmee krijgt die je hele website in handen.

Wat moet je doen?

Zet tweestapsverificatie aan voor iedereen die kan inloggen. Laat het inlogscherm ook blokkeren na een paar foute pogingen.

Wie: **je webbouwer**

</> VOOR JE WEBBOUWER

```
/wp-login.php en /xmlrpc.php: geen rate limiting of lockout (500 pogingen in 4 minuten, geen blokkade).
Advies: 2FA voor alle beheerders, lockout na 5 pogingen, xmlrpc.php uitschakelen als het niet nodig is.
```

MIDDEL

4 Nepmail uit jouw naam wordt niet tegengehouden

Wanneer **deze maand**

Wat er aan de hand is

Iedereen kan e-mail versturen die van jouw bedrijf lijkt te komen. Je domeinnaam vertelt mailservers niet dat ze zulke mail moeten weigeren.

Wat kan er gebeuren?

Oplichters kunnen je klanten een nepfactuur sturen met jouw naam en e-mailadres erop. Voor je klanten is het verschil niet te zien.

Wat moet je doen?

Vraag je mailprovider of hostingbedrijf om dit in te stellen (het heet ‘DMARC’). Eerst een paar weken meten, daarna stap voor stap strenger.

Wie: **je mailprovider of hostingbedrijf**

</> VOOR JE WEBBOUWER

```
_dmarc.[jouwbedrijf].nl: geen record. SPF aanwezig (~all), DKIM aanwezig.
Begin met "v=DMARC1; p=none; rua=mailto:dmarc@[jouwbedrijf].nl" en ga na 2 tot 4 weken naar
p=quarantine.
```

LAAG

5 Foutmeldingen verklappen hoe je website in elkaar zit

Wanneer **bij het volgende onderhoud**

Wat er aan de hand is

Gaat er iets mis op je website, dan toont die een foutmelding met technische details, zoals de mappen op de server.

Wat kan er gebeuren?

Een aanvaller heeft daar niet direct iets aan, maar het maakt een aanval wel makkelijker.

Wat moet je doen?

Laat je webbouwer de foutmeldingen voor bezoekers uitzetten. Je webbouwer kan ze dan nog wel zien.

Wie: **je webbouwer**

</> VOOR JE WEBBOUWER

```
WP_DEBUG en WP_DEBUG_DISPLAY staan aan; PHP-fouten tonen serverpaden (/var/www/vhosts/…).
Zet in wp-config.php: define('WP_DEBUG_DISPLAY', false); en log naar een bestand buiten de webroot.
```

3 Wat je nu doet

Begin bovenaan en vink af wat klaar is. Stuur dit rapport naar je webbouwer: die vindt bij elk punt de technische details.

	PUNT	WAT	WIE	WANNEER	
☐	1	Oude back-up verwijderen en nagaan of die is gedownload	Webbouwer	Vandaag	HOOG
☐	3	Inlogscherm beveiligen met tweestapsverificatie	Webbouwer	Deze maand	MIDDEL
☐	2	Plug-in bijwerken en maandelijkse updates afspreken	Webbouwer	Deze maand	MIDDEL
☐	4	Nepmail uit jouw naam laten tegenhouden	Mailprovider of hostingbedrijf	Deze maand	MIDDEL
☐	5	Foutmeldingen voor bezoekers uitzetten	Webbouwer	Volgend onderhoud	LAAG

Over deze test

Deze pentest is uitgevoerd door een ethisch hacker van onze partner Gomanche, met je schriftelijke toestemming. Alleen Nederlanders, geen offshoring, en elke specialist is gescreend. We hebben geprobeerd binnen te komen zoals een echte aanvaller dat zou doen, zonder iets te veranderen of mee te nemen.

Is alles opgelost? Doe dan de gratis check op isjewebsiteveilig.nl om de buitenkant opnieuw te controleren.

Liever dat wij het oplossen?

We lopen de actielijst met je door en regelen het met je webbouwer, of doen het zelf.

Mail [e-mailadres]
Bel [telefoonnummer]