# Advies security scan voor WebwinkelKeur leden

Normaal gesproken staat er een virusscanner op jouw computer maar wie controleert de beveiliging van jouw webwinkel? De meeste mensen staan niet stil bij de gevolgen en kosten die gemaakt moeten worden wanneer een webwinkel wordt gehackt. Zodra dit gebeurd kun je een paar dagen geen omzet genereren, je bouwt reputatieschade op en je bent kosten kwijt om het probleem op te lossen. Om dit te voorkomen is de veiligheid van jouw webwinkel essentieel!

Een geldig SSL certificaat is een eerste stap in de goede richting. Als je echt zeker wilt zijn van de veiligheid op jouw website kun je een premie uitloven voor hackers (bijvoorbeeld via www.hackerone.com). Zij dringen jouw website binnen en proberen op alle manieren om te bewijzen dat jouw webwinkel niet veilig genoeg is. Vervolgens leggen ze uit hoe ze dat gedaan hebben. Met die kennis kun jij de veiligheid van jouw webwinkel verbeteren. Dat is natuurlijk een goede optie maar om zo'n premie uit te loven heb je behoorlijk wat tijd, programmeerkennis en zelfvertrouwen nodig!

We weten dat een hacker inschakelen een grote stap is, gelukkig is er een makkelijkere manier. Je kunt namelijk jouw webwinkel laten monitoren door gebruik te maken van een security scan. Tot eind 2020 boden we onze leden de security scan van Provensec. Omdat we het belangrijk vinden om ons op dit gebied te ontwikkelen hebben we alternatieven getest. Hieronder vind je de resultaten van ons gebruikersonderzoek.

## Opzet gebruikersonderzoek

Er zijn veel aanbieders van security scans. Enkele bekende aanbieders zijn: Qualys, Trust Guard, McAfee Secure, Detectify, Sectigo, Pentest Tools en Securi. Om de beste keuze te maken hebben we hen allen uitgenodigd om hun product te presenteren. Trust Guard en Sectigo toonden interesse. Na een demonstratie zijn een we een gebruikerstest gestart en hebben we een goede vergelijking gemaakt.

Aan deze test hebben 5 webwinkeliers en 2 medewerkers van WebwinkelKeur deelgenomen. Deze groep is groot genoeg om ons een goede indruk te geven. Ook kunnen we door deze testgroep een goed advies aan onze leden geven. De testgroep is naar onze mening wel te klein om een harde conclusie te trekken. Hieronder vind je de resultaten van de test.

We hebben onze testers gevraagd om hun huidige security scan Provensec op 3 punten te vergelijken met Trust Guard en Sectigo;

- Is het makkelijk om je aan te melden en de security scan in te stellen?
- Is het duidelijk wat er wordt gemonitord en met welke frequentie dat gebeurd?
- Indien er een security issue is gevonden:
    - Hoe werd je op de hoogte gebracht van het issue? E-mail / sms / overig.
    - Begrijp je het issue dat is gerapporteerd?
    - Is het duidelijk wat je moet doen met het gerapporteerde issue?

# Resultaten gebruikersonderzoek

## Is het makkelijk om je aan te melden en het systeem in te stellen?

| Security Scan | Cijfer | Toelichting |
|---|---|---|
| Trust Guard | 9 | Trust Guard oogt een tikkeltje ouderwets, maar is wel overzichtelijk. Een medewerker neemt contact op om je persoonlijk te begeleiden bij de aanmelding. De mails zijn erg duidelijk en het dashboard is overzichtelijk, we zouden er zelf ook wel uitkomen, maar is wel prettig dat iemand je aan de hand neemt en dat je vervolgens een direct aanspreekpunt hebt. |
| Sectigo | 8 | Je krijgt inloggegevens per email en de aanmelding verloopt intuïtief. Het dashboard oogt modern. “Add a site to monitor” en klaar ben je. |
| Provensec | 3 | Je krijgt inloggegevens per email en de aanmelding verloopt intuïtief. Echter later blijkt dat je een aantal instellingen moet veranderen om goed gebruik te maken van deze scan (instellen van alerts en de frequentie van testen). |

## Is het duidelijk wat er wordt gemonitord en met welke frequentie?

| Security Scan | Cijfer | Toelichting |
|---|---|---|
| Trust Guard | 9 | “Was erg duidelijk wat de scan ging doen.“ en de reactie van een andere testgebruiker: “Gewoon duidelijke uitleg, je ziet wat er wordt gemonitord, wat er misschien verkeerd gaat.” |
| Provensec | 8 | Per monitor (vulnarability, mallware en uptime) is er een duidelijk overzicht van de recente scans en resultaten. Helaas is er geen totaal overzicht. |
| Sectigo | 4 | Een beknopt overzicht met domeinnamen, laatste scan datum en de status van de laatste scan. De testers vonden deze informatie te summier, je krijgt geen gevoel bij wat er getest is. |

## Hoe nuttig zijn de scanresultaten?

| Security Scan | Cijfer | Toelichting |
|---|---|---|
| Trust Guard | 7 | Je kunt instellen dat je van Trust Guard een mail ontvangt als er vulnerabilities zijn gevonden. Wij hebben gevraagd deze instelling de default optie te maken, waaraan zij gehoor hebben gegeven door de software aan te passen. Top!<br><br>De gevonden issues worden gecategoriseerd op de ernst van de vulnerability: info, low, medium, high en serious. Als er medium issues of hoger worden gerapporteerd, dan is je domein voor de test gezakt.<br><br>Per issue is er een rapport met een uitleg en een oplossing. Deze uitleg is behoorlijk technisch. De meeste webwinkeliers zullen dit rapport moeten doorsturen naar zijn of haar developer.<br><br>Als je developer het er niet mee eens is, dan sta je als ondernemer tussen twee vuren. Wat ook gebeurde: “None of these are really important. It's just some notices about certain settings we have, but none of those really need fixing. They are typical notices you get from security scan software.” Als ondernemer ontbreekt het je vervolgens aan de kennis om een goed oordeel te vormen. Ga je uit van de expertise van je developer die al jaren voor je goed werk levert? Of ga je uit van de test standaarden van externe scan? Een verdomd lastig dilemma.<br><br>Als een developer aangeeft dat een vulnerability niet terecht is, dan kun je markeren dat het een ‘false positive’ betreft. Vervolgens zal het team van Trust Guard onderzoeken. Als deze geaccordeerd wordt zal dit issue geen gefaalde test meer veroorzaken. |
| Provensec | 5 | Vergelijkbaar als bij Trust Guard alleen dan zonder de default mail functionaliteit en zonder de mogelijkheid om gerapporteerde issues als “false positives” aan te merken. |
| Sectigo | | Van alle test domeinen samen is er 1 keer een issue gerapporteerd. Een malware bestand. Daarvan werd een mail gestuurd met de bestandsnaam. Erg duidelijk, op basis van dit proces zou Sectigo het hoogste scoren.<br><br>Echter zijn er sterke twijfels ontstaan of de scan van Sectigo wel alle issues vind. De andere scans hebben vele medium en small issues gerapporteerd. We hebben de belangrijkste issues voorgelegd aan Sectigo en gevraagd om een uitleg waarom die niet gerapporteerd zijn. Helaas hebben we daarop nog geen antwoord ontvangen en kunnen we geen conclusies trekken. Het zou namelijk kunnen zijn dat de scan andere zaken test, we deze niet goed hadden ingesteld of dat de gemelde issues geen serieuze issues zijn. |

## Overige overwegingen

Trust Guard heeft ons positief verrast door de door ons aangedragen verbeterpunten meteen door te voeren in hun software. Wij werken graag samen met partijen die snel kunnen schakelen.

Sectigo bied naast de security scan ook veel andere handige functionaliteiten zoals back ups, SSL certificaten en ‘remediation’. Bij remediation worden issues die geconstateerd zijn opgelost. Zo is het gerapporteerde malware bestand door hun verwijderd van de server. Hiervoor dien je wel toegang te geven tot je FTP/SFTP.

Provensec beëindigd haar dienstverlening per 1 januari 2021. Om die reden kunnen deze scan niet langer aanbieden.

De prijs is natuurlijk ook belangrijk. Provensec en Sectigo zijn te gebruiken voor minder dan €10 per maand. De prijs van Trust Guard bedraagt tussen de €9 en €23 per maand afhankelijk van de scanfrequentie.

## Conclusie en aanbod naar onze leden

Uit onze gebruikerstest is Trust Guard een duidelijke winnaar. Zij maken vooral het verschil doordat ze persoonlijke service en uitgebreide informatievoorziening bieden. Er is nog wel verbetering mogelijk wat betreft de manier waarop de gevonden issues gerapporteerd worden.

Helaas hebben we van Sectigo nog geen reactie gehad op de belangrijkste gevonden issues door de andere scans. Daardoor kunnen we geen uitspraak doen over de kwaliteit van Sectigo.

Vanaf 1 januari 2021 adviseren wij Trust Guard als alternatief voor de security scan van Provensec. Daarbij zullen wij werken aan een integratie waardoor je na een succesvolle security test bij Trust Guard beloond wordt met onze “veilig browsen” badge op je profielpagina. Wanneer je jouw domein minstens 1 keer per week laat controleren wordt je gekwalificeerd voor de ‘’SUPER veilig browsen’’ badge.

Omdat je lid van WebwinkelKeur bent ontvang je 25% eenmalige korting en 15% structurele korting bij Trust Guard. 14 dagen testen is sowieso gratis. Je kunt je aanmelden voor deze actie in het menu ‘aanbiedingen’ wanneer je inlogt op jouw Dashboard van WebwinkelKeur.