AVG PAKKET

Met een WordPress website kiest men voor veel gebruiksgemak, net als 39% van de andere websites wereldwijd. Om een website aan de AVG te laten voldoen, moet men met een aantal zaken rekening houden... De AVG, ofwel Algemene Verordening Persoonsgegevens is de Europese privacy wet, die per 25 mei 2018 van kracht is en het nodige stof doet opwaaien.

Adequate beveiliging

Zo schrijft de AVG voor dat persoonsgegevens een adequate beveiliging moeten hebben. Dus papieren patiëntendossiers achter gesloten deuren, computers met versleutelde opslag en online moeten websites aan wettelijke voorwaarden voldoen.

SSL is niet genoeg

Webdesigners schrijven daarom SSL verbindingen voor om sites te beveiligen. Dit zorgt echter alleen maar voor een beveiliging tussen de bezoekers en de website. Wanneer een site al gehackt is, zijn de persoonsgegevens van eigen mensen en van klanten in gevaar.

Hackers in de praktijk

Vanwege hackers moeten de updates van computers en websites voortaan actief bijgehouden worden. Beveiligingsbedrijf Sucuri berekende dat 71% van de hacks in 2017 via plugins en thema’s van WordPress verlopen. Het grootste deel van de hacks van WordPress vond plaats via versies die niet up to date waren.

Dit moet u regelen

- SSL verbinding voor de website

- Een up to date 'privacy verklaring'

Zie de privacy verklaring generator:
https://veiliginternetten.nl/privacyverklaring/

Organisatorische maatregelen:

- Hoe vaak wordt een website geüpdate? (minimaal 4 en bij voorkeur 12 keren per jaar)

- Wie doen dit? (uzelf?) (Of) (https://projectattis.nl)

- Welke beveiliging heeft men? (Afhankelijk van de door u gekozen hosting)

- En wat als er iets mis gaat?

Websites 'AVG-proof-maken'

Neem dit AVG pakket goed door en indien u ons voor onderdelen hiervan in wilt zetten neem even contact met ons op.

avg@projectattis.nl

073 6129 777 / 06 341 320 80