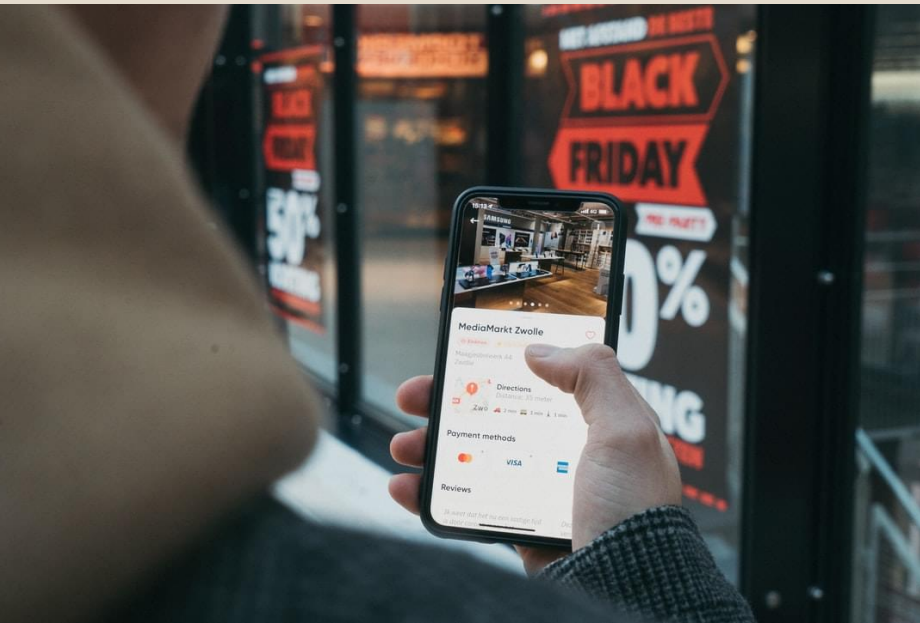


Cyberweerbaarheid eCommerce Nederland



85% van de websites van eCommerce-bedrijven vertoont kwetsbaarheden

Ons onderzoek naar de cyberweerbaarheid van websites van eCommerce-bedrijven (webwinkels) toont aan dat 83 van de 98 onderzochte websites gemiddelde tot grote kwetsbaarheden vertoont.

Cybercriminelen kunnen dan ook schadelijke acties uitvoeren, zoals het overnemen van websites of het stelen van gevoelige klantinformatie zoals wachtwoorden of bankgegevens. Het verbeteren van de cyberweerbaarheid zou dan ook een hoge prioriteit moeten hebben bij deze bedrijven.

De kwetsbaarheid van een website is doorgaans een goede indicatie van de mate waarin aandacht is besteed aan de algehele beveiliging van de IT-omgeving. Daarnaast zijn websites vaak de eerste plek waar aanvallers zoeken naar potentiële beveiligingslekken. Hierbij kijken ze voornamelijk naar het gemak om een IT-omgeving te hacken, niet direct naar de waarde. Ze vormen dus ook wel het ‘topje van de ijsberg’ binnen de IT-beveiliging.

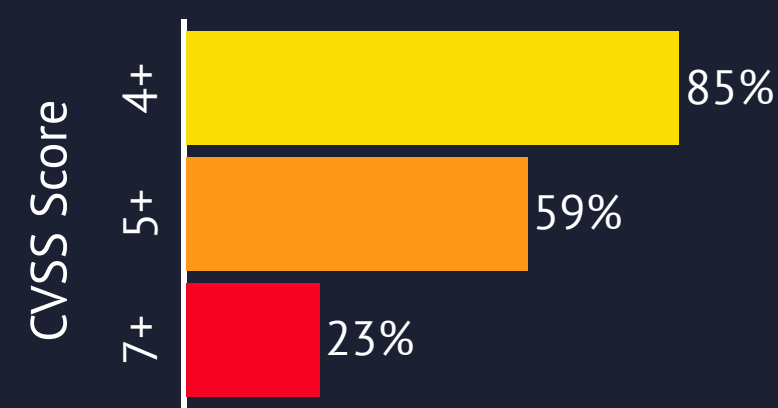


Van de 20 geautomatiseerde, niet invasieve tests, die wij uitvoeren op een website om deze te controleren op mogelijke kwetsbaarheden **falen er bijna 4**, waarbij er ook websites zijn waar zelfs 8 van de 20 tests niet succesvol zijn.



De zwakste schakel is bepalend in de beveiliging van de website en IT-omgeving. Onze scan laat zien dat er, op een schaal van 0 tot 10, waarbij 0 aangeeft dat een site veilig is en 10 betekent dat de site kritische kwetsbaarheden bevat, een **gemiddelde kwetsbaarheidsscore is van 5,12**. Daarbij scoort deze branche ondergemiddeld ten opzichte van andere branches.

Aantal websites vs. kwetsbaarheidsscores



De resultaten van onze tests worden gemeten volgens het CVSS-framework* dat de kwetsbaarheidsscore bepaalt naar aanleiding van de karakteristieken en ernst van de gevonden kwetsbaarheden.

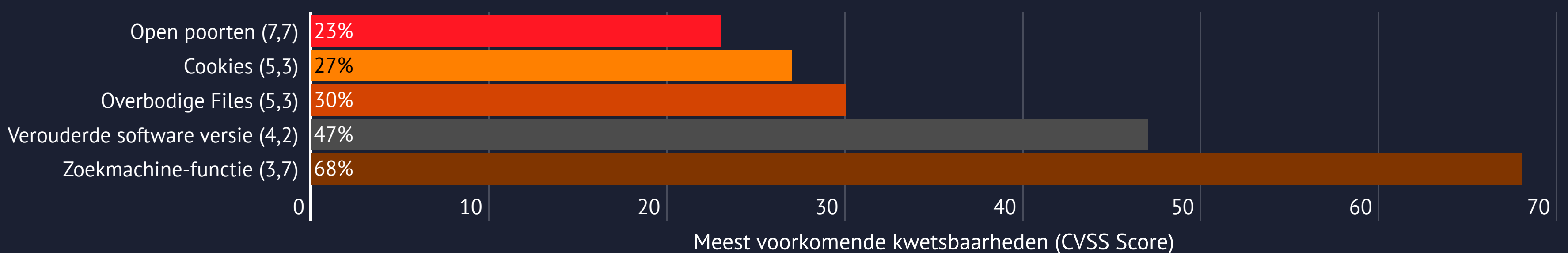
Scores tussen 4 en 7 worden gezien als gemiddeld kwetsbaar en boven de 7 als zeer kwetsbaar. We zien dus dat bij 85% van de websites een kwetsbaarheid is gevonden die als gemiddeld beoordeeld wordt, maar ook dat **23% van de sites zeer kwetsbaar is**.

*Het Common Vulnerability Scoring System (CVSS) is een open en algemeen geaccepteerd framework voor het kwalificeren van softwarekwetsbaarheden.

Meest gevonden kwetsbaarheden

Met behulp van onze geautomatiseerde scan kijken we naar een 20-tal kwetsbaarheden. In onderstaand overzicht zijn de 5 meest voorkomende kwetsbaarheden weergegeven. Hierbij vallen een aantal zaken op:

1. Bijna **1 op de 4 websites heeft poorten open staan**, dit naast de gangbare poorten voor webverkeer. Dit is te vergelijken met een open raam of deur bij een kantoor of woonhuis. Hierdoor kan een hacker toegang krijgen tot het netwerk en gevoelige data.
2. Er wordt op veel domeinen **teveel gevoelige informatie weggegeven** waar hackers gebruik van kunnen maken.
3. De ondersteunende software die gebruikt wordt voor de websites wordt **slecht geüpdatet**, waarbij vaak nog met oudere softwareversies gewerkt wordt.



Advies om cyberweerbaarheid te verhogen



Advies is om **overbodige poorten**, naast de noodzakelijke, **te sluiten** en alleen verkeer toe te staan van vertrouwde bronnen door bijvoorbeeld whitelisting.



Er worden continu nieuwe kwetsbaarheden gevonden in software, recentelijk bijvoorbeeld in Microsoft Exchange. Software- en hardware-bedrijven brengen dan ook regelmatig nieuwe updates uit om deze veiliger te maken. **Ons advies is om altijd hard- en software te updaten naar de nieuwste versie.**



Zorg dat de configuratie van websites geen gevoelige data bevat, en **zorg dat communicatie tussen website en browser veilig is**.

Hoe Sygnius kan helpen?

IT-omgevingen, websites en software veranderen continu en het is dan ook belangrijk voor bedrijven om doorlopend op de hoogte te blijven van de cyberweerbaarheid van die IT-omgeving of websites. Vanuit Sygnius helpen we bedrijven om inzicht te krijgen in de cyberweerbaarheid en daarop passende maatregelen te nemen. Geen overkill, maar passend bij het bedrijf, waarbij we samen kijken naar de kans op en mogelijke gevolgen van een cyberaanval.

Neem voor meer informatie contact met ons op: E-mail: info@sygnius.nl / Telefoon: 06 - 8115 2826 / Website: www.sygnius.nl