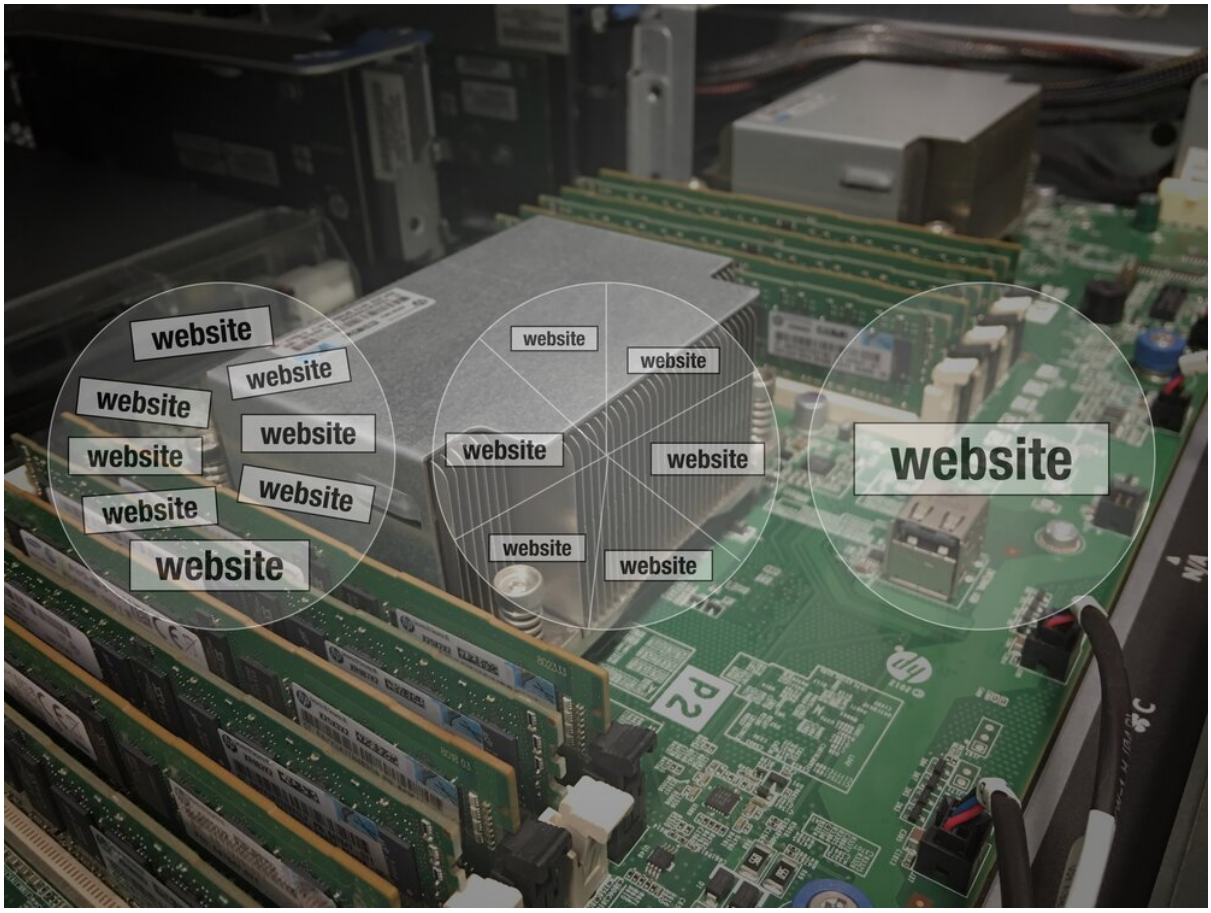
Veiligheidsrisico's bij shared hosting

Openstaande poorten en ongebruikte netwerkgerichte services in overweging nemen

Willem L. Middelkoop
28 feb. 2019



Mensen betalen mij om ze te hacken, mits ik uitleg hoe het gedaan is, zodat toekomstige hacks voorkomen kunnen worden. Als beveiligingsconsultant scan ik op zwakke plekken in de apps, webshops en websites van mijn klanten. Heel vaak begint een hack door het misbruiken van een beveiligingslek dat op afstand zichtbaar is. Lees verder om te leren hoe hackers beveiligingslekken vinden en wat je kunt doen om ze te dichten.

Om een app, webshop of website te hacken, richten hackers zich vaak op de servers die deze hosten. Om uit te leggen waarom hackers dit doen, moet je eerst begrijpen wat hosting is en welke soorten hosting er zijn.

Wat is hosting?

Hosting is een dienst waarmee je je app, webshop of website beschikbaar kunt maken op het internet. Hosting gebeurt met behulp van speciale computers, servers genaamd. Wanneer iemand je websiteadres in zijn browser typt, maakt zijn apparaat verbinding met jouw server.

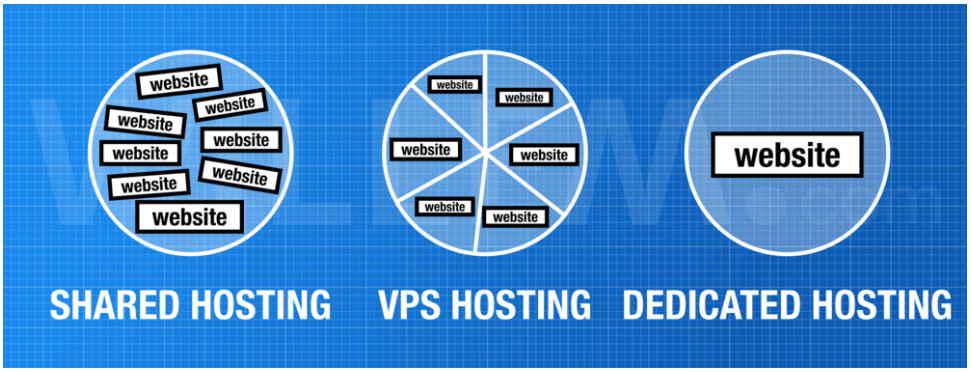
Als hackers een server onder controle kunnen krijgen, hebben ze toegang tot alle informatie die erop staat en kunnen ze deze manipuleren. Bovendien kunnen ze de netwerk- en rekencapaciteit van de server misbruiken om kwaad te doen. Dit wil je echt niet...

Een typische server in het datacenter, een fysieke machine die apps, webshops en websites kan hosten

Verschillende soorten hosting

Je app, webshop of website kan op verschillende manieren worden gehost. Elke soort hosting heeft verschillende beveiligingsoverwegingen, maar het is relatief eenvoudig te begrijpen, aangezien het allemaal neerkomt op hoe de fysieke server (in het datacenter) wordt gedeeld tussen de websites.

Webhostingbedrijven exploiteren meestal meerdere servers en verdelen hun capaciteit over het aantal websites dat hosting nodig heeft. Eén grote server kan gemakkelijk meerdere websites hosten, afhankelijk van de hoeveelheid verkeer die de app, webshop of website heeft.



Verschillende soorten hosting: Shared hosting, VPS hosting en dedicated hosting gevisualiseerd (een cirkel die een fysieke server voorstelt)

Er zijn drie verschillende soorten hosting:

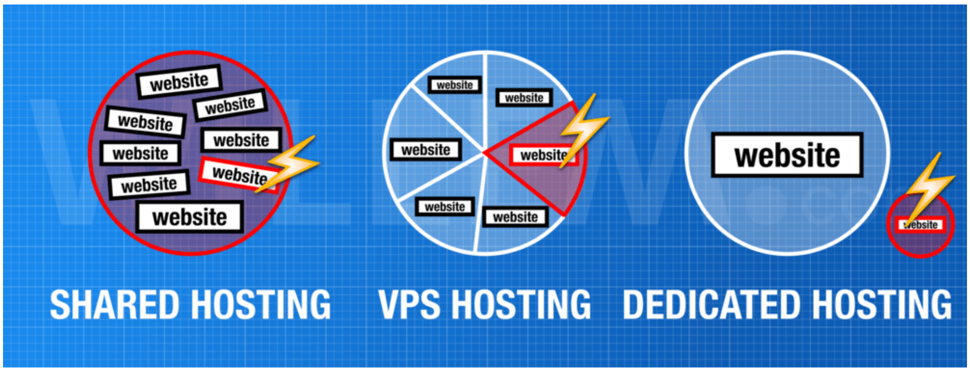
- **shared hosting**: De server draait meerdere websites door het besturingssysteem, geheugen, processorkernen en harde schijfruimte te delen. Er zijn geen harde scheidingen tussen de websites.
- **VPS hosting**: De fysieke server draait meerdere virtuele privéservers (VPS) die allemaal hun eigen besturingssysteem en hun eigen deel van het geheugen, de processorkracht en de opslag hebben. Een enkele VPS kan worden geconfigureerd om één of een paar (gerelateerde) websites te draaien. Door de harde scheiding tussen de VPS-instanties is het voor hackers erg moeilijk om van de ene VPS naar de andere te komen.
- **dedicated hosting**: De fysieke server draait slechts één website. Niets wordt gedeeld, alle resources zijn toegewijd aan één app, webshop of website. Door deze fysieke scheiding word je niet getroffen door hacks van andere websites.

Waarschuwing: "Cloud Hosting" is vaak omgedoopte shared hosting

Het is belangrijk om te begrijpen dat de meeste moderne "Cloud Hosting" eigenlijk *shared hosting* is met een mooie naam. Webdesignbureaus configureren vaak hun dedicated of virtuele privéserver om shared hosting aan hun klanten te verkopen. Dus, tenzij je je eigen VPS of dedicated server beheert, is de kans groot dat je op shared hosting zit.

Beveiligingsproblemen bij shared hosting

De beveiligingsrisico's van shared hosting komen voort uit het gedeelde karakter ervan. Wanneer een van de websites op dezelfde server als die van jou wordt gehackt, is de kans groot dat jouw website ook wordt getroffen. In deze situatie zijn beveiligingsmaatregelen die op je eigen website worden toegepast mogelijk niet voldoende om deze te beschermen tegen hackers.



Besmettelijk effect van een gehackte website (rood geeft problemen aan)

Gedeeld IP-adres

Bovendien betekent shared hosting meestal dat alle websites hetzelfde IP-adres delen. Je krijgt problemen als een andere website betrokken is bij slechte praktijken, zoals het versturen van spam of het hosten van illegale inhoud. Dit kan ertoe leiden dat je website op een zwarte lijst komt te staan, wordt geblokkeerd of lager scoort in zoekmachines.

Prestaties

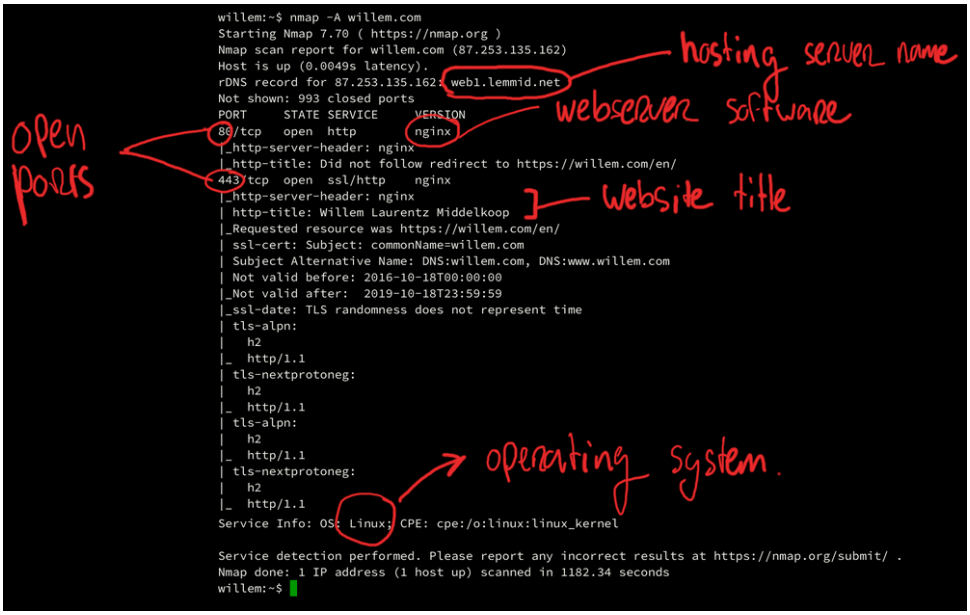
Als je bedenkt dat hostingbedrijven meestal honderden - soms zelfs duizenden (!) - websites op dezelfde shared server plaatsen, begrijp je waarom dit de kans op hacking vergroot. Naast beveiligingsproblemen heeft een shared hostingdienst ook invloed op de prestaties van je website, omdat deze moet concurreren met andere websites om dezelfde beperkte hoeveelheid serverresources. Als een van de andere websites extreem veel verkeer ervaart, kan dit ook jouw app, webshop of website vertragen!

Gedeelde netwerkgerichte diensten

Een ander probleem met shared hosting is dat de server meestal veel netwerkgerichte diensten ingeschakeld heeft, zoals een web-, mail-, FTP- en databaseservice. Deze services zijn beschikbaar via open poorten. Het is een slechte gewoonte om alle poorten overal open te hebben staan, omdat het de services die op die poorten luisteren blootstelt aan exploits. Firewalls kunnen beperken wat er mag verbinden met een bepaalde poort, maar in een shared hostingomgeving zijn deze beperkingen vaak niet erg streng (vanwege de vele verschillende dingen die op dezelfde server worden gehost).

Een app, webshop of website hacken

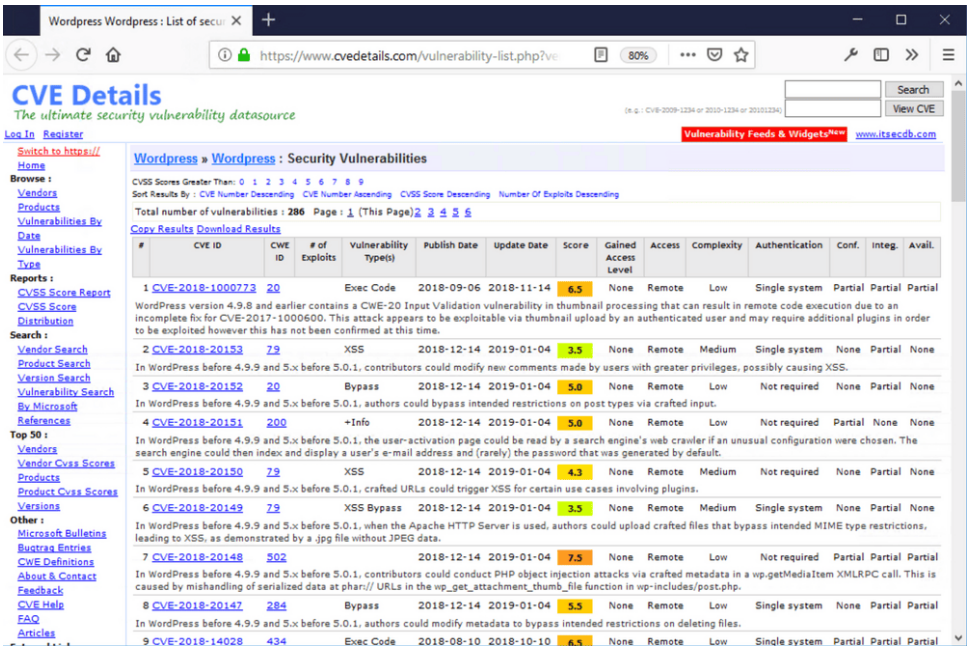
Om jouw app, webshop of website te hacken, kan een hacker je hostingserver scannen op open poorten, waarbij de verschillende services die op de server draaien worden geïdentificeerd. Het unix-programma *nmap* wordt hiervoor vaak gebruikt. De hacker maakt verbinding met de service die luistert op open poorten om erachter te komen welk programma het is.



Nmap gebruiken om een hosting server te scannen, netwerkgerichte services en open poorten identificeren

Deze informatie kan worden gebruikt om te controleren of actieve netwerkservices bekende beveiligingsproblemen hebben. Er zijn online bibliotheken waar deze zwakke punten kunnen worden opgezocht op softwarenaam en -versie. Het vinden van een bekende zwakke plek is zo eenvoudig als een Google query. Als er een bestaande zwakke plek wordt gevonden, kan de hacker deze gebruiken om toegang te krijgen tot de server.

Door het IP-adres van de hostingserver te controleren, kan de hacker bepalen of de server wordt gedeeld met andere apps, webshops of websites. Het is mogelijk (met behulp van omgekeerde DNS-lookups) om alle websites op te sommen die op dezelfde server worden gehost. Hoewel die van jou up-to-date en veilig kan zijn, kunnen anderen op dezelfde server verouderde software draaien (met beveiligingsproblemen). Veelgebruikte websitesoftware is goed gedocumenteerd, oudere versies van PHP en WordPress staan erom bekend dat ze ernstige beveiligingsproblemen hebben.



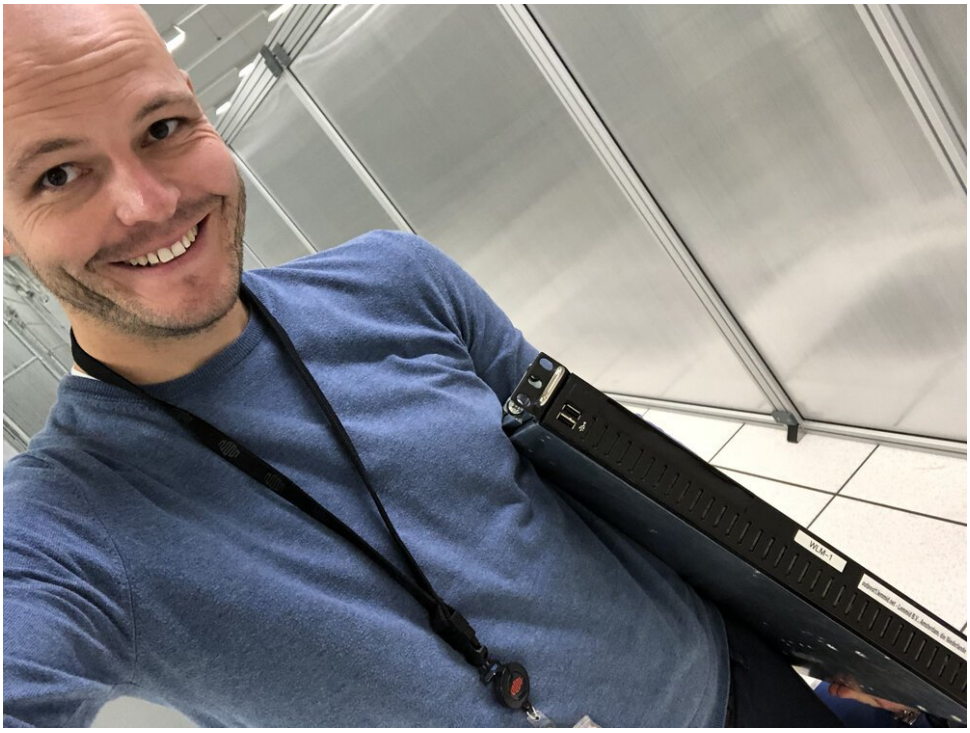
Zodra een hacker weet welke software je website gebruikt, is het makkelijk om bekende beveiligingslekken op te zoeken met behulp van databases zoals cvedetails.com

Conclusie

De beste manier om je app, webshop of website te beveiligen, is door de blootstelling aan exploits zoveel mogelijk te beperken. Het is essentieel om je websitesoftware up-to-date te houden, maar het is misschien niet voldoende als je hosting gedeeld is.

Om te voorkomen dat andere hacks van invloed zijn op je app, webshop of website, moet je overwegen om deze te hosten op een dedicated fysieke of virtuele server met een eigen IP-adres. Je kunt de beveiliging vervolgens aanscherpen door open poorten te filteren en ongebruikte netwerkgerichte services uit te schakelen.

Op deze manier verklein je wat cybersecurity-experts het ”aanvalsoppervlak” noemen. Hoe kleiner het is, hoe gemakkelijker het wordt om het te verdedigen - veel succes en houd in gedachten dat hulp beschikbaar is!



Houd in gedachten dat er hulp beschikbaar is - ik weet mijn weg in servers en cybersecurity