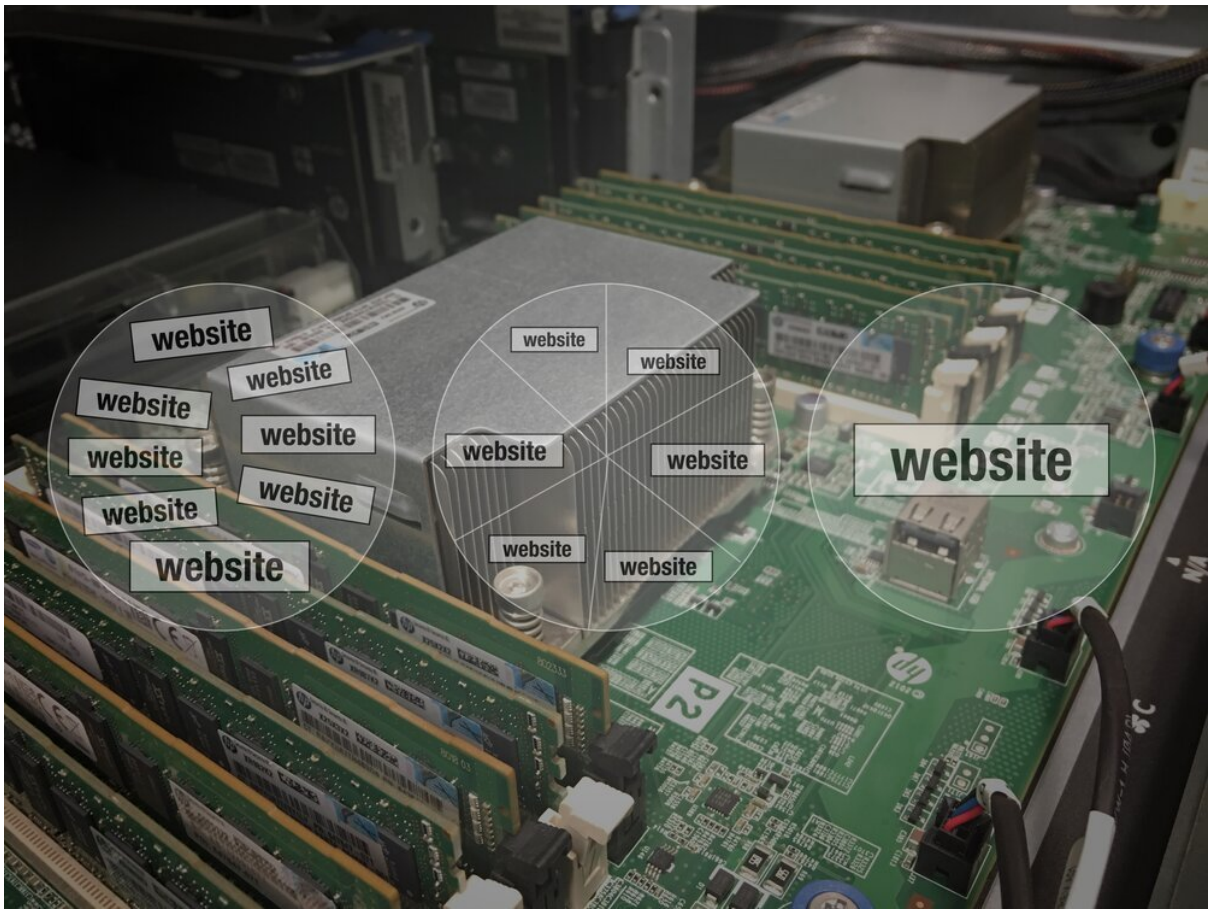
Sicherheitsbedenken im Shared Hosting verstehen

Berücksichtigung offener Ports und ungenutzter Netzwerkdienste

Willem L. Middelkoop
Feb. 28, 2019



Man bezahlt mich dafür, Systeme zu hacken, vorausgesetzt, ich erkläre, wie es gemacht wurde, damit zukünftige Hacks verhindert werden können. Als Sicherheitsberater suche ich nach Schwachstellen in den Apps, Webshops und Websites meiner Kunden. Sehr oft beginnt ein Hack mit der Ausnutzung einer Sicherheitslücke, die aus der Ferne sichtbar ist. Lesen Sie weiter, um zu erfahren, wie Hacker Sicherheitslücken finden und was Sie tun können, um sie zu schließen.

Um eine App, einen Webshop oder eine Website zu hacken, greifen Hacker oft die Server an, auf denen diese gehostet werden. Um zu erklären, warum Hacker dies tun, müssen Sie zunächst verstehen, was Hosting ist und welche Arten von Hosting es gibt.

Was ist Hosting?

Hosting ist ein Dienst, der es Ihnen ermöglicht, Ihre App, Ihren Webshop oder Ihre Website im Internet verfügbar zu machen. Hosting erfolgt über spezielle Computer, sogenannte Server. Wenn jemand Ihre Website-Adresse in seinen Browser eingibt, verbindet sich sein Gerät mit Ihrem Server.

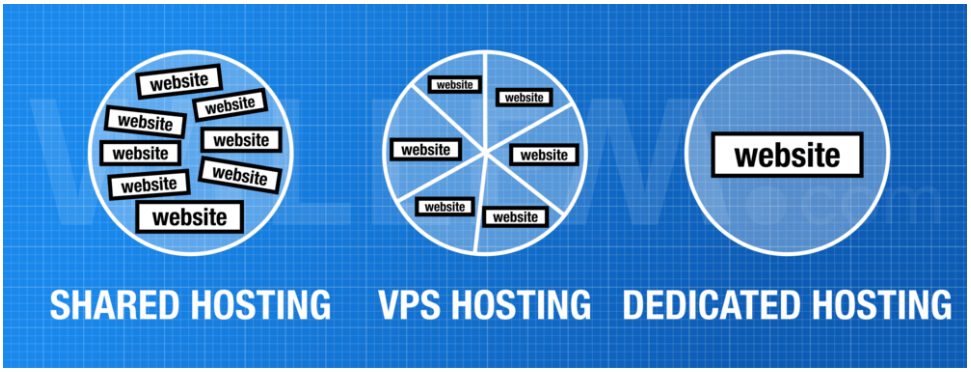
Wenn Hacker die Kontrolle über einen Server übernehmen können, können sie auf alle darauf befindlichen Informationen zugreifen und diese manipulieren. Darüber hinaus können sie die Netzwerk- und Rechenkapazität des Servers missbrauchen, um schädliche Dinge zu tun. Das wollen Sie wirklich nicht...

Ein typischer Server im Rechenzentrum, eine physische Maschine, die Apps, Webshops und Webseiten hosten kann

Verschiedene Arten von Hosting

Ihre App, Ihr Webshop oder Ihre Website kann auf verschiedene Arten gehostet werden. Jede Art von Hosting hat unterschiedliche Sicherheitsaspekte, aber es ist relativ einfach zu verstehen, da es darauf ankommt, wie der physische Server (im Rechenzentrum) zwischen den Websites geteilt wird.

Webhosting-Unternehmen betreiben in der Regel mehrere Server und teilen deren Kapazität auf die Anzahl der Websites auf, die Hosting benötigen. Ein großer Server kann problemlos mehrere Websites hosten, abhängig vom Traffic der App, des Webshops oder der Website.



Verschiedene Arten von Hosting: Shared Hosting, VPS Hosting und Dedicated Hosting visualisiert (ein Kreis, der einen physischen Server darstellt)

Es gibt drei verschiedene Arten von Hosting:

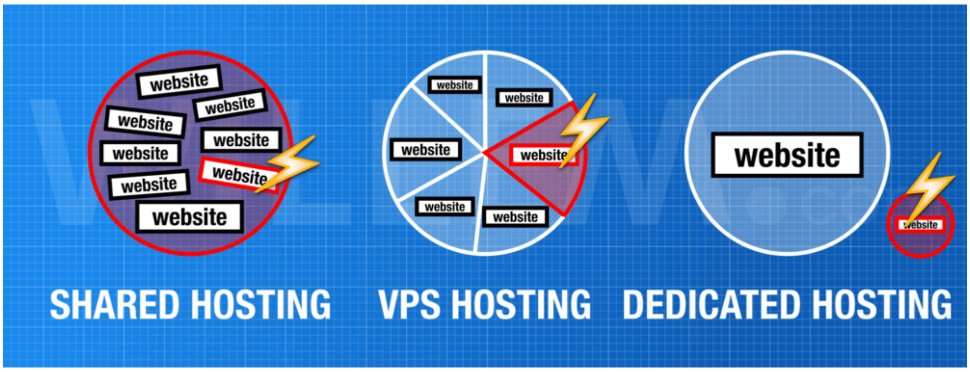
- **Shared Hosting**: Der Server betreibt mehrere Websites, indem er sich das Betriebssystem, den Speicher, die Prozessorkerne und den Festplattenspeicher teilt. Es gibt keine strikte Trennung zwischen den Websites.
- **VPS-Hosting**: Der physische Server betreibt mehrere virtuelle private Server (VPS), die jeweils über ein eigenes Betriebssystem und einen eigenen Anteil an Speicher, Prozessorleistung und Speicherplatz verfügen. Ein einzelner VPS kann so konfiguriert werden, dass er eine oder mehrere (verwandte) Websites betreibt. Aufgrund der strikten Trennung zwischen den VPS-Instanzen ist es für Hacker sehr schwierig, von einem VPS zum anderen zu gelangen.
- **Dediziertes Hosting**: Der physische Server betreibt nur eine Website. Nichts wird geteilt, alle Ressourcen sind einer App, einem Webshop oder einer Website zugeordnet. Aufgrund dieser physischen Trennung sind Sie nicht von Hacks anderer Websites betroffen.

Warnung: "Cloud Hosting" ist oft umbenanntes Shared Hosting

Es ist wichtig zu verstehen, dass das meiste moderne "Cloud Hosting" eigentlich *Shared Hosting* mit einem schicken Namen ist. Webdesign-Büros konfigurieren oft ihren dedizierten oder virtuellen privaten Server, um Shared Hosting an ihre Kunden zu verkaufen. Wenn Sie also nicht Ihren eigenen VPS oder dedizierten Server betreiben, befinden Sie sich wahrscheinlich auf einem Shared Hosting.

Sicherheitsbedenken bei Shared Hosting

Die Sicherheitsrisiken von Shared Hosting ergeben sich aus der gemeinsamen Nutzung. Wenn eine der Websites auf demselben Server wie Ihre gehackt wird, besteht eine hohe Wahrscheinlichkeit, dass auch Ihre Website betroffen ist. In dieser Situation reichen die auf Ihrer eigenen Website angewandten Sicherheitsmaßnahmen möglicherweise nicht aus, um sie vor Hackern zu schützen.



Ansteckungseffekt einer gehackten Webseite (rot zeigt Probleme an)

Gemeinsame IP-Adresse

Darüber hinaus bedeutet Shared Hosting in der Regel, dass sich alle Websites dieselbe IP-Adresse teilen. Sie werden Probleme bekommen, wenn eine andere Website in schlechte Praktiken verwickelt ist, wie z. B. das Versenden von Spam-Mails oder das Hosten illegaler Inhalte. Dies könnte dazu führen, dass Ihre Website auf die schwarze Liste gesetzt, blockiert oder in den Suchmaschinen-Rankings herabgestuft wird.

Leistung

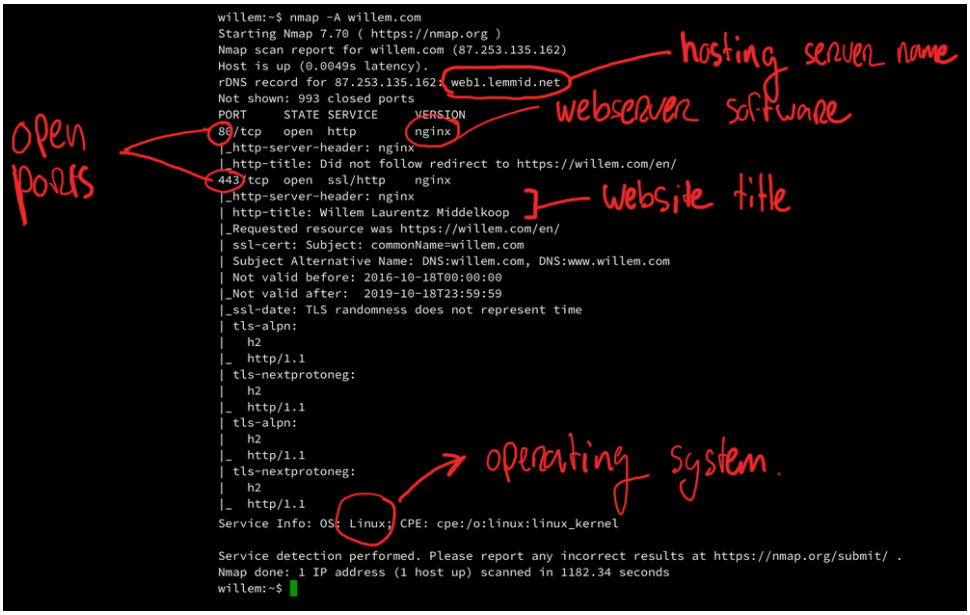
Wenn Sie bedenken, dass Hosting-Unternehmen in der Regel Hunderte - manchmal sogar Tausende (!) - von Websites auf demselben Shared Server unterbringen, werden Sie verstehen, warum dies die Wahrscheinlichkeit erhöht, gehackt zu werden. Neben den Sicherheitsproblemen beeinträchtigt ein Shared Hosting-Dienst auch die Leistung Ihrer Website, da sie mit anderen Websites um die gleichen begrenzten Serverressourcen konkurrieren muss. Wenn eine der anderen Websites extremen Traffic erlebt, könnte dies auch Ihre App, Ihren Webshop oder Ihre Website verlangsamen!

Gemeinsame Netzwerkdienste

Ein weiteres Problem bei Shared Hosting ist, dass der Server in der Regel viele Netzwerkdienste aktiviert hat, wie z. B. einen Web-, Mail-, FTP- und Datenbankdienst. Diese Dienste sind über offene Ports verfügbar. Es ist schlechte Praxis, alle Ports für alle offen zu haben, da dies die Dienste, die auf diesen Ports lauschen, für Exploits zugänglich macht. Firewalls können einschränken, was eine Verbindung zu einem bestimmten Port herstellen darf, aber in einer Shared-Hosting-Umgebung sind diese Einschränkungen oft nicht sehr streng (wegen der vielen verschiedenen Dinge, die auf demselben Server gehostet werden).

Hacken einer App, eines Webshops oder einer Website

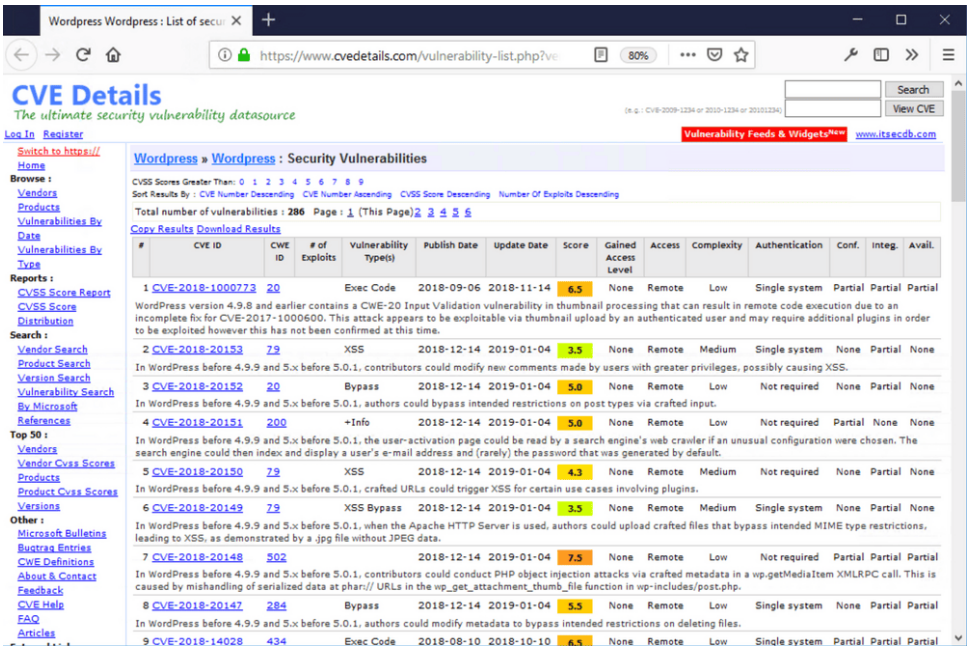
Um Ihre App, Ihren Webshop oder Ihre Website zu hacken, kann ein Hacker Ihren Hosting-Server nach offenen Ports scannen und so die verschiedenen Dienste identifizieren, die auf dem Server laufen. Das Unix-Programm *nmap* wird oft dafür verwendet. Der Hacker verbindet sich mit dem Dienst, der auf offenen Ports lauscht, um herauszufinden, um welches Programm es sich handelt.



Verwendung von nmap zum Scannen eines Hosting-Servers, Identifizierung von Netzwerkdiensten und offenen Ports

Diese Informationen können verwendet werden, um zu überprüfen, ob laufende Netzwerkdienste bekannte Sicherheitslücken aufweisen. Es gibt Online-Bibliotheken, in denen diese Schwachstellen nach Softwarename und -version gesucht werden können. Das Finden einer bekannten Schwachstelle ist so einfach wie eine Google Abfrage. Wenn eine vorhandene Schwachstelle gefunden wird, kann der Hacker diese nutzen, um sich Zugang zum Server zu verschaffen.

Durch die Überprüfung der IP-Adresse des Hosting-Servers kann der Hacker feststellen, ob der Server mit anderen Apps, Webshops oder Websites geteilt wird. Es ist möglich (mittels Reverse-DNS-Lookups), alle Websites aufzulisten, die auf demselben Server gehostet werden. Während Ihre Website möglicherweise aktuell und sicher ist, könnten andere auf demselben Server veraltete Software (mit Sicherheitslücken) verwenden. Gängige Website-Software ist gut dokumentiert, ältere Versionen von PHP und WordPress sind dafür bekannt, ernsthafte Sicherheitsprobleme zu haben.



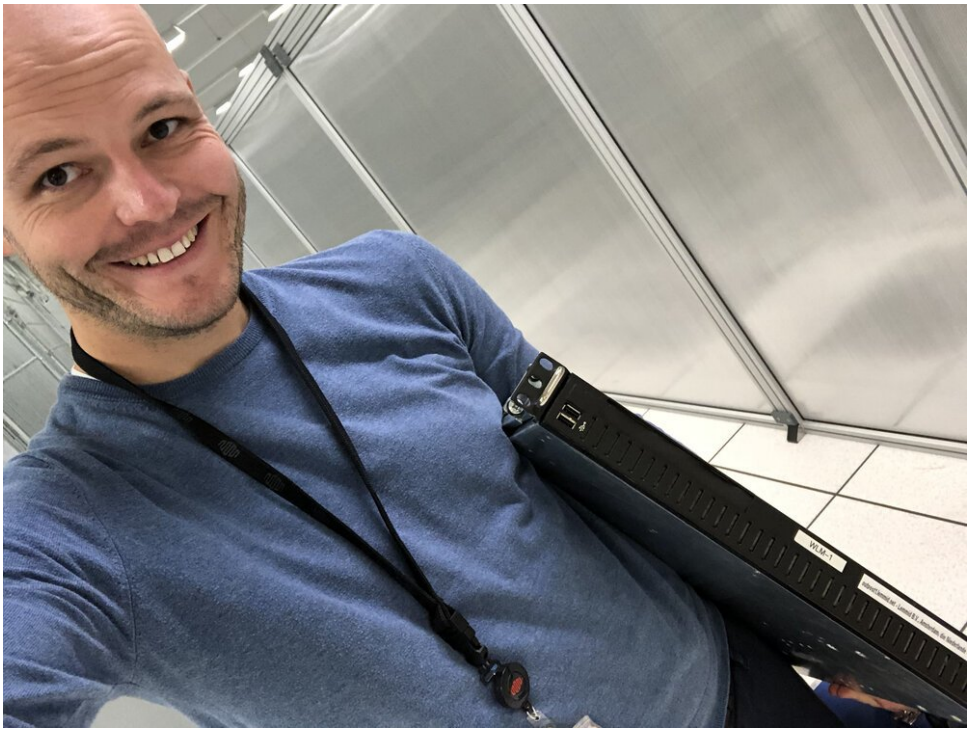
Sobald ein Hacker weiß, welche Software Ihre Webseite verwendet, ist es einfach, bekannte Sicherheitslücken mithilfe von Datenbanken wie cvedetails.com zu finden

Fazit

Der beste Weg, Ihre App, Ihren Webshop oder Ihre Website zu schützen, besteht darin, die Angriffsfläche so weit wie möglich zu reduzieren. Es ist wichtig, Ihre Website-Software auf dem neuesten Stand zu halten, aber das reicht möglicherweise nicht aus, wenn Ihr Hosting gemeinsam genutzt wird.

Um zu verhindern, dass andere Hacks Ihre App, Ihren Webshop oder Ihre Website beeinträchtigen, sollten Sie in Erwägung ziehen, sie auf einem dedizierten physischen oder virtuellen Server mit einer eigenen IP-Adresse zu hosten. Sie können dann die Sicherheit erhöhen, indem Sie offene Ports filtern und ungenutzte Netzwerkdienste abschalten.

Auf diese Weise reduzieren Sie das, was Cybersicherheitsexperten die ”Angriffsfläche” nennen. Je kleiner sie ist, desto leichter lässt sie sich verteidigen - viel Glück und denken Sie daran, dass Hilfe verfügbar ist!



Denken Sie daran, dass Hilfe verfügbar ist - Ich kenne mich mit Servern und Cybersicherheit aus