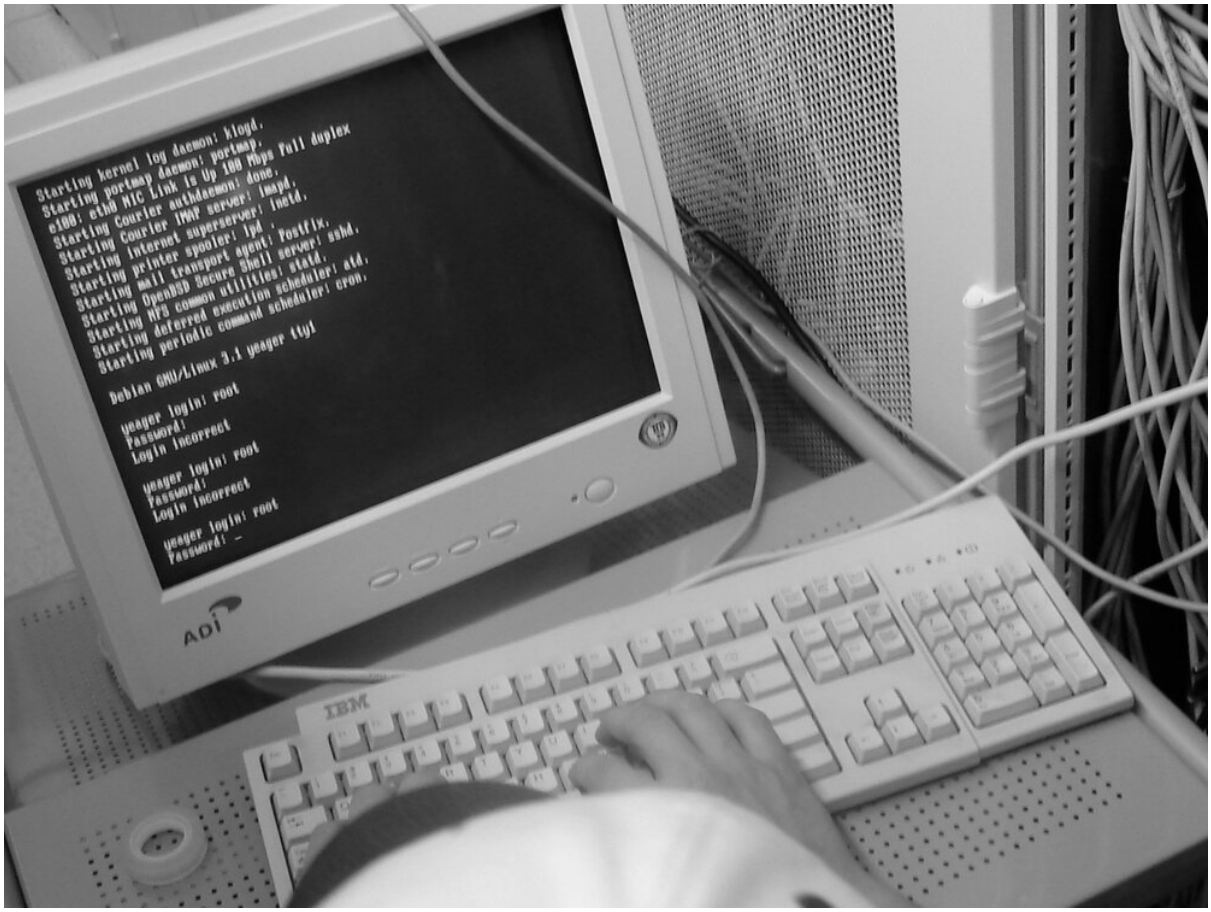
Cybersicherheit: 5 einfache Tipps zum Schutz Ihres Servers vor Hackern

Best Practices zur Server-Härtung für Windows und Linux

Willem L. Middelkoop
Mar. 10, 2018



Diese Woche wurde einer meiner Kunden gehackt und bat mich um Nothilfe bei der Sicherung seiner Serverinfrastruktur. Es handelte sich um einen Webserver, der WordPress-Websites auf Apache (mit PHP/MySQL) betrieb, darunter auch einige Webshops mit Kundendaten. Dieser Hack hätte mit den folgenden Best Practices leicht verhindert werden können. Ist *Ihr* Server sicher?

Das Rechenzentrum ist der Ort, an dem sich Ihr Server befindet. Auch wenn es physisch sicher sein mag, sollten Sie auch die Software überprüfen!

1) Weniger Software installieren

Cybersicherheit ist schwierig genug, Sie sollten es sich einfacher machen, indem Sie weniger Software installieren. Weniger Programme, Dienste und Plugins bedeuten weniger Dinge, über die Sie sich Sorgen machen müssen. In der Cybersicherheitsterminologie wird dies als Reduzierung der Angriffsfläche bezeichnet.

Reduzieren Sie Ihre Angriffsfläche, indem Sie:

- **mit einem minimalen Basissystem beginnen**: Beginnen Sie nicht mit einem aufgeblähten Betriebssystem, sondern mit so wenig wie möglich und behalten Sie den Überblick über die Dinge, die Sie hinzufügen.
- **nur das installieren, was Sie unbedingt benötigen**: Installieren Sie nur Tools, Plugins, Add-ons und Programme, die Sie wirklich - wirklich - brauchen. Seien Sie hart und entschlossen: Weniger ist mehr!
- **Abhängigkeiten von Dingen überprüfen, die Sie installieren**: Wenn Sie etwas installieren, stellen Sie sicher, dass Sie die Abhängigkeiten überprüfen; Software benötigt oft andere Software (die Sie nicht unbedingt wollen).

2) Alle Netzwerkports schließen, diejenigen filtern, die Sie nicht blockieren können

Firewalls werden verwendet, um den Netzwerkverkehr zu filtern und sind auf den meisten Betriebssystemen als Standardsystemsoftware verfügbar. Begrenzen Sie die Öffnungen, die Hacker zu Ihrem Server haben.

Die Firewall-Konfiguration sollte:

- **eine Standardrichtlinie des Blockierens übernehmen:** Die meisten Betriebssysteme erlauben standardmäßig alles. Drehen Sie dies um und blockieren Sie alles außer der Art von Verkehr, die Sie erwarten und benötigen.
- **eingehenden und ausgehenden Verkehr überprüfen:** Filtern Sie eingehenden und ausgehenden Netzwerkverkehr. Dies macht es Hackern viel schwerer, einzudringen (und im unglücklichen Fall eines erfolgreichen Hacks wieder herauszukommen).
- **offene Ports filtern:** Sichern Sie offene Netzwerkports, indem Sie den Verkehr basierend auf der Quelle (IP-Adresse) und/oder dem Status filtern, erlauben Sie nur Verkehr von dort, wo Sie ihn erwarten.

3) Alle Versionsinformationen ausblenden

Die Software, die Ihr Server ausführt, ist versioniert, oft eine Nummer, die das genaue Datum angibt, an dem sie erstellt wurde. Hacker können diese Versionsinformationen verwenden, um bekannte Sicherheitsprobleme, Schwachstellen und Schwächen nachzuschlagen.

Hören Sie auf, Hackern zu helfen, indem Sie Versionsinformationen entfernen von:

- **Webservern:** Apache, NGINX, Microsoft Internet Information Services, etc. Überprüfen Sie Ihren Server durch Analyse der HTTP-Header.
- **Mailservern:** Postfix, Exim, Dovecot, Sendmail, etc. Oft kommunizieren diese Server ihre Version in einem "Hello Banner", das direkt nach dem Aufbau einer Verbindung über SMTP, IMAP, POP3 angezeigt wird.
- **Websprachen:** PHP, .NET, Java, etc. Manchmal fügen diese Frameworks und Skriptsprachen ihren eigenen HTTP-Header ("x-powered-by") mit Versionsinformationen hinzu.
- **WordPress:** Plugins, Themes, Formulare, Galerien, Webshops, etc. Versionsinformationen sind oft in der HTML-Ausgabe oder in Dateinamen von CSS, JavaScript und Bildern enthalten.
- **Dateiservern:** FTP, SFTP, WebDav, etc. Diese Server kommunizieren ihre Versionsinformationen in ihrer Begrüßung, die direkt nach der Verbindung, oft vor der Authentifizierung, angezeigt wird.
- **SSH:** Wussten Sie, dass OpenSSH standardmäßig Betriebssystem-Versionsinformationen übermittelt?

4) Verwenden Sie Zertifikat-/Schlüsselauthentifizierung anstelle von Passwörtern

Wenn passwortbasierte Anmeldungen erlaubt sind, können Hacker wiederholt versuchen, auf den Server zuzugreifen. Mit moderner Rechenleistung ist es einfach, dieses Raten zu automatisieren, indem Kombination nach Kombination ausprobiert wird, bis das richtige Passwort gefunden ist (Brute-Forcing).

Sichere Authentifizierung durch:

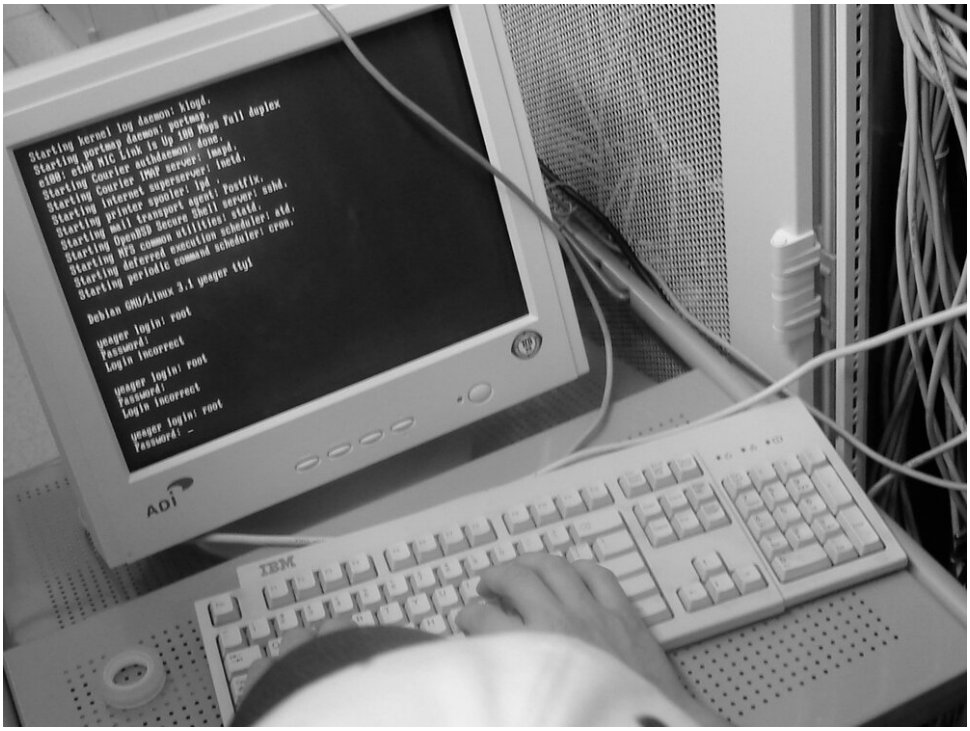
- **Verwendung der SSH-Schlüsselauthentifizierung:** Ein SSH-Schlüssel ist viel länger als ein normales Passwort und enthält andere Zeichen als gewöhnliche lesbare Buchstaben und Zahlen. Dies führt zu mehr möglichen Kombinationen, was es für Hacker exponentiell schwieriger macht, den richtigen Schlüssel zu finden.
- **Begrenzung der Authentifizierungsrate:** Künstlich die Passwort-/Schlüsselprüfung verlangsamen, um die Geschwindigkeit des automatisierten Ratens zu reduzieren.
- **Blockieren des automatisierten Ratens:** IP-Adressen ausschließen, wenn die Anmeldung nicht erfolgreich war.

5) Regelmäßig überprüfen und aktualisieren

Heutzutage läuft das meiste Hacking automatisiert ab, Bots scannen ständig jeden Server und jede Website nach Angriffsmöglichkeiten. Es ist keine Frage *OB* sie Sie finden werden, sondern *WANN*.

Kümmern Sie sich um Ihren Server, indem Sie:

- **seine Protokolle überprüfen:** Potenzielle Probleme werden oft sichtbar, bevor wirklich schlimme Dinge passiert sind. Überprüfen Sie die Serverprotokolle auf Fehler und Anomalien; oft sind sie frühe Anzeichen für Probleme.
- **nach Updates suchen:** Entweder mithilfe der Software auf Ihrem Server oder durch Überprüfen der Website des Herstellers/der Software.
- **regelmäßig aktualisieren:** Warten Sie nicht, bis es zu spät ist, installieren Sie Updates so schnell wie möglich (aber *nachdem* Sie sie getestet haben!).



Überprüfen Sie Ihren Server regelmäßig – oder finden Sie jemanden, der das für Sie erledigt.

Fazit

Wenn Sie diese Maßnahmen umsetzen, können Sie die Cybersicherheit Ihres Servers erheblich verbessern. Der Schutz Ihres Servers bedeutet mehr Sicherheit für Ihr Unternehmen, Ihre Organisation und die Daten Ihrer Kunden.

Kein (vernünftiger) Sicherheitsberater wird Ihnen Garantien geben, mit genügend Ressourcen und Entschlossenheit werden Hacks immer möglich sein. Seien Sie vorbereitet, indem Sie Backups erstellen und Ihre Daten verschlüsseln.

Hoffentlich helfen Ihnen diese Tipps. Wenn Sie zusätzliche Hilfe benötigen, finden Sie meine Kontaktinformationen hier oder sehen Sie sich meine Cybersicherheitsdienste an.