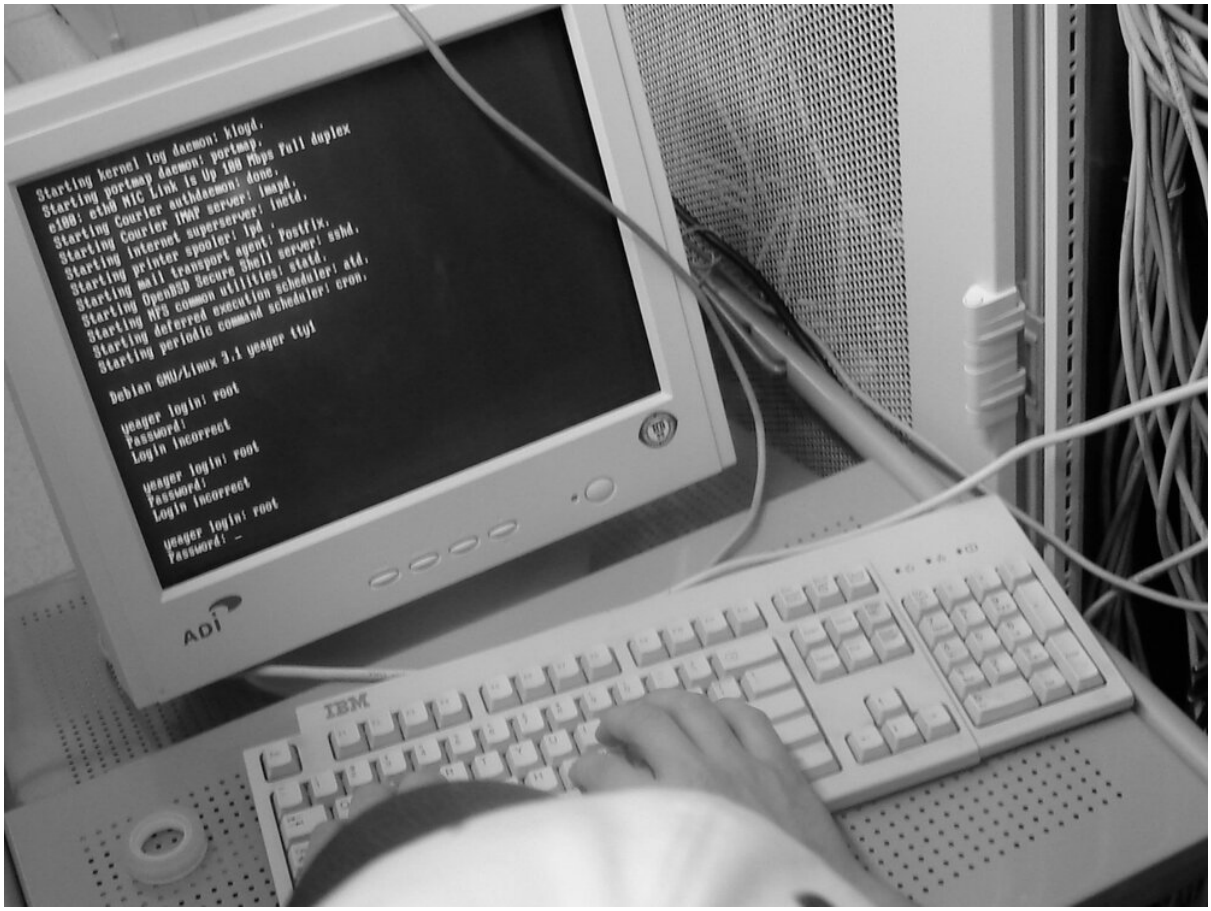
Cyberbeveiliging: 5 eenvoudige tips om je server te beschermen tegen hackers

Beveiliging van servers - best practices voor Windows en Linux

Willem L. Middelkoop
10 mrt. 2018



Deze week werd één van mijn klanten gehackt en vroeg mij om noodhulp bij het beveiligen van hun serverinfrastructuur. Het betrof een webserver die WordPress websites draaide op Apache (met PHP/MySQL), inclusief een paar webshops met klantgegevens. Deze hack had eenvoudig voorkomen kunnen worden met de volgende best practices, is *jouw* server wel veilig?

Het datacenter is waar je server staat. Ook al is het fysiek misschien wel beveiligd, je moet ook de software controleren!

1) Installeer minder software

Cyberbeveiliging is al lastig genoeg, maak het jezelf makkelijker door minder software te installeren. Minder programma's, services, plugins betekent minder om je zorgen over te maken. In cyberbeveiligingsterminologie wordt dit het verkleinen van de aanvalsvector genoemd.

Verklein je aanvalsvector door:

- **te beginnen met een minimaal basissysteem**: begin niet met een volledig en opgeblazen besturingssysteem, start met zo min mogelijk en houd bij wat je toevoegt
- **alleen te installeren wat je absoluut nodig hebt**: installeer tools, plugins, add-ons en programma's die je echt - echt - nodig hebt. Wees streng en vastberaden: minder is meer!
- **afhankelijkheden te controleren van dingen die je installeert**: Als je iets installeert, controleer dan de afhankelijkheden; software vereist vaak andere software (die je niet per se wilt)

2) Sluit alle netwerkpoorten, filter die je niet kunt blokkeren

Firewalls worden gebruikt om netwerkverkeer te filteren en zijn beschikbaar als standaard systeem software op de meeste besturingssystemen. Beperk de openingen die hackers hebben naar jouw server.

Firewall configuratie zou:

- **een standaardbeleid van blokkeren moeten hanteren:** De meeste besturingssystemen staan standaard alles toe. Draai dit om en blokkeer alles behalve het soort verkeer dat je verwacht en nodig hebt.
- **zowel inkomend als uitgaand verkeer moeten controleren:** Filter inkomend en uitgaand netwerkverkeer. Dit maakt het voor hackers veel moeilijker om binnen te komen (en eruit te komen - in het ongelukkige geval van een succesvolle hack).
- **open poorten moeten filteren:** Beveilig open netwerkpoorten door verkeer te filteren op basis van bron (IP-adres) en/of status, sta alleen verkeer toe van waar je het verwacht.

3) Verberg alle versie-informatie

De software die jouw server gebruikt, heeft een versie, vaak een nummer dat de exacte datum aangeeft waarop deze is gebouwd. Hackers kunnen deze versie-informatie gebruiken om bekende beveiligingsproblemen, kwetsbaarheden en zwakke punten op te zoeken.

Stop met het helpen van hackers door versie-informatie te verwijderen van:

- **webservers:** Apache, NGINX, Microsoft Internet Information Services, etc. Controleer je server door de HTTP-headers te analyseren.
- **mailservers:** Postfix, Exim, Dovecot, Sendmail, etc. Vaak communiceren deze servers hun versie in een ”hello banner”, die direct na het tot stand brengen van een verbinding met behulp van SMTP, IMAP, POP3 wordt weergegeven.
- **web talen:** PHP, .NET, Java, etc. Soms voegen deze frameworks en scripttalen hun eigen HTTP-header (”x-powered-by”) toe met versie-informatie.
- **WordPress:** plugins, thema's, formulieren, galerijen, webshops, etc. Versie-informatie is vaak opgenomen in HTML-output of in bestandsnamen van CSS, JavaScript en afbeeldingen.
- **bestandsservers:** FTP, SFTP, WebDav, etc. Deze servers communiceren hun versie-informatie in hun begroetingsbericht, dat direct na het verbinden wordt weergegeven, vaak vóór authenticatie.
- **SSH:** Wist je dat OpenSSH standaard informatie over de besturingssysteemversie communiceert?

4) Gebruik certificaat/sleutel authenticatie in plaats van wachtwoorden

Als aanmeldingen op basis van wachtwoorden zijn toegestaan, kunnen hackers herhaaldelijk proberen toegang te krijgen tot de server. Met moderne rekenkracht is het gemakkelijk om dit raden te automatiseren door combinatie na combinatie te proberen totdat het juiste wachtwoord is gevonden (brute forcing).

Beveilig authenticatie door:

- **SSH-sleutelauthenticatie te gebruiken:** een SSH-sleutel is veel langer dan een normaal wachtwoord en bevat andere tekens dan gewone leesbare letters en cijfers. Dit resulteert in meer mogelijke combinaties, waardoor het exponentieel moeilijker wordt voor hackers om de juiste sleutel te vinden.
- **authenticatiesnelheid te beperken**: Maak het controleren van wachtwoorden/sleutels kunstmatig langzamer, waardoor de snelheid van geautomatiseerd raden wordt verminderd.
- **geautomatiseerd raden te blokkeren**: Sluit IP-adressen uit als ze niet succesvol hebben ingelogd.

5) Controleer en update regelmatig

Het meeste hacken is tegenwoordig geautomatiseerd, bots scannen constant elke server en website op mogelijkheden tot uitbuiting. Het is geen vraag *OF* ze je zullen vinden, maar *WANNEER*.

Zorg voor je server door:

- **de logboeken te controleren:** potentiële problemen worden vaak zichtbaar voordat er echt slechte dingen zijn gebeurd. Controleer de serverlogboeken op fouten en afwijkingen; vaak zijn dit vroege tekenen van problemen.
- **te controleren op updates:** door de software op je server te gebruiken of door de website van de leverancier/software te controleren.
- **regelmatig te updaten:** wacht niet tot het te laat is, installeer updates zo snel mogelijk (maar *nadat* je ze hebt getest!)

Controleer je server regelmatig - of zoek iemand die dit voor je doet.

Conclusie

Als je deze maatregelen implementeert, kun je de cyberbeveiliging van je server aanzienlijk verbeteren. Het beschermen van je server betekent betere veiligheid voor je bedrijf, je organisatie en de gegevens van je klanten.

Geen (gezonde) beveiligingsconsultant zal je garanties bieden, met voldoende middelen en vastberadenheid zullen hacks altijd mogelijk zijn. Wees voorbereid door back-ups te maken en je gegevens te versleutelen.

Hopelijk helpen deze tips je, als je extra hulp nodig hebt, kun je mijn contactgegevens hier vinden of mijn cyber_security_services bekijken.