Der er en del omtale af at websites, der er baseret på WordPress, for tiden er udsat for mange angreb fra hackere.

Metoden er tilsyneladende at forsøge at logge ind med kombinationer af hackede brugernavne og password, der florerer på nettet.

Angrebene sker via såkaldte *botnet*. Angrebene kommer fra maskiner over hele verden, som hackerne kontrollerer. Tusindvis af danskere er med i disse botnet – uden at vide det.

Hvad kan man gøre, for at holde hackerne ude?

Man kan ikke undgå angreb, men man kan gøre meget for at hindre dem i at trænge ind.

Her er tre tip, der øger sikkerheden betragteligt.

Undgå usikre brugernavne og adgangskoder

Som standard er brugernavnet for en WordPress-administrator *admin*. Hackerne satser derfor ofte på at forsøge med dette brugernavn.

Det er derfor en god ide at droppe admin som brugernavn: Opret en ny administrator med et andet navn, og slet admin.

Adgangskoden bør være på 8-10 bogstaver. Læs om valg af adgangskoder her.

Blokér for mange logins

WordPress tillader at man prøver at logge ind i én uendelighed. Derfor er det en god ide at bruge et plugin, der begrænser antallet af mulige logins.

Brug fx Limit Login Attempts. Med dette plugin kan man sætte en grænse på fx fem loginforsøg fra én IP-adresse, før der spærres for login-forsøg i en periode.

Man kan også få adviseringer om loginforsøg via email og meget andet.

Blokér for logins fra udlandet

Da langt de fleste angreb sker fra maskiner i udlandet, er det en kæmpe fordel, hvis man kan sortere alle disse angreb fra.

Og det kan man.

Der findes flere plugins, som tackler dette problem:

Admin Block Country

IP2Location Country Blocker

Da jeg indsatte et sådant plugin, havde jeg haft 3.000 loginforsøg på et par timer. Det faldt stort set til nul med det samme.

Flyt login-side

Man logger normalt ind på en side, der hedder ../wp-admin, så det er den, hackerne angriber.

Med plugin'et *Rename wp-login.php,* kan man flytte login til en anden adresse, som hackerne ikke kender, og det virker ret effektiv.

Hackerne vil opleve at siden ikke findes, og så vil de kaste sig over en anden WordPress-installation.

Plugin'et vedligeholdes ikke, men det fungerer stadig uden de store problemer.

(Revideret januar 2015, oprindelig artikel juni 2013).