

Ein Content-Management-System muss besonders gegen Angriffe geschützt werden. Die Änderung von Inhalten durch Unbefugte ist ein absolutes Worst-Case-Szenario. Leider kommt in der Praxis immer wieder ein *Defacement*, also das Verändern von Inhalten durch Dritte, vor.

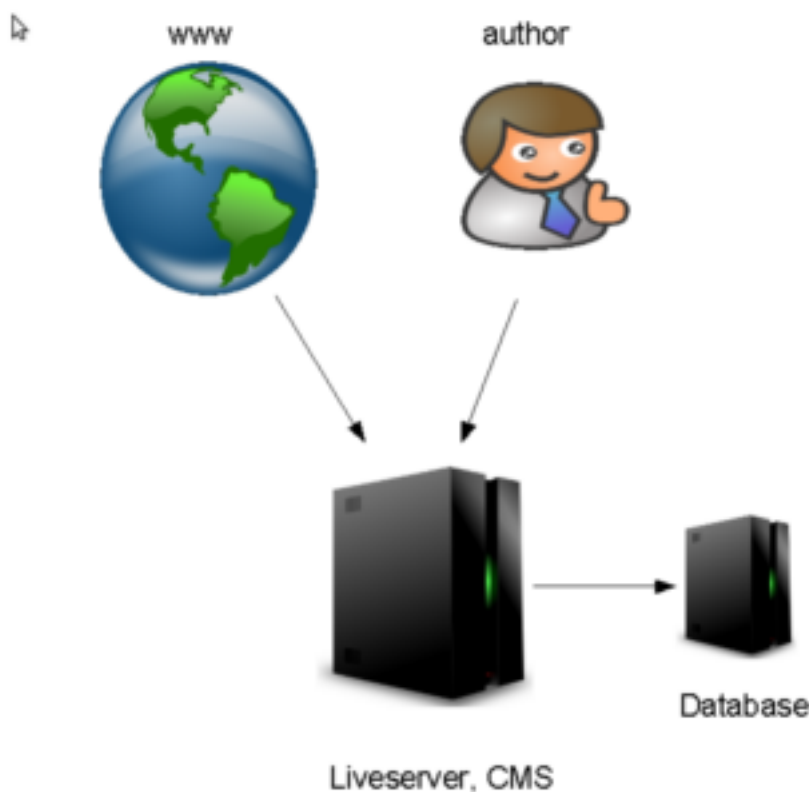
Die meisten Systeme sind mittlerweile gut abgesichert. Dennoch wird ein besonderer Angriffspunkt meist vergessen: Wenn das CMS aus dem Internet erreichbar ist, dann ist das System direkt Angriffen ausgesetzt. Stets muss auf Aktualität und Einspielen von Sicherheitspatches geachtet werden.

Um Sicherheit zu gewinnen ist es das Beste, die Gefahr durch Angriffe von außen auf das CMS netzwerktechnisch gar nicht zu ermöglichen. Die Lösung lautet: Statifizierung. Durch die Generierung von statischen Seiten ist das CMS auf dem Internet gar nicht zwingend erreichbar, sondern ausschließlich nur besonderen Benutzergruppen, z.B. im Intranet oder VPN erreichbar. Der Webserver bleibt schlank und überdies wird die Performance und Skalierbarkeit erhöht.

Beispiel für angriffsbefährdete Live-CMS

Clips are licenced under Creative commons

Unsecured CMS

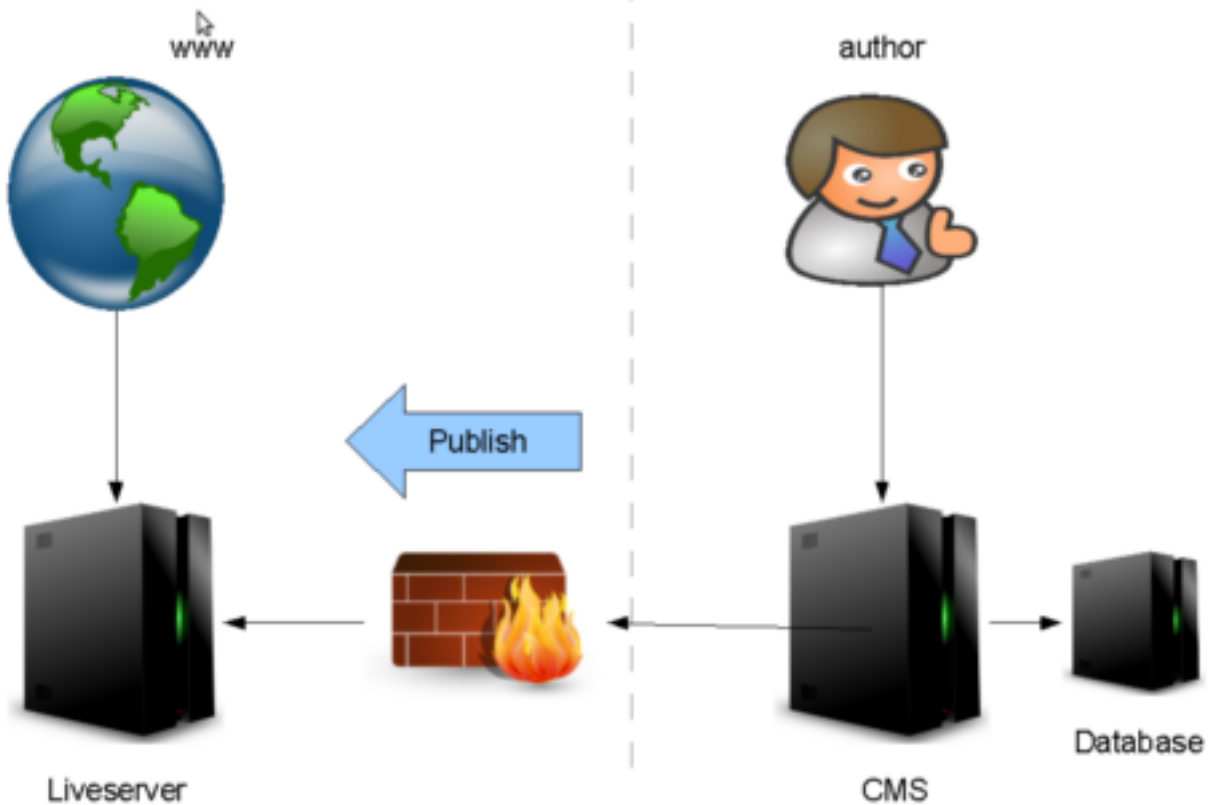


Das CMS liefert die Seiten on-the-fly aus. Möglicherweise gibt es einen eigenen Bereich für Administratoren oder Redakteure, aber das System ist aus dem Internet erreichbar. Da zum Betrieb meist eine Datenbank eingesetzt wird, steigt die Komplexität und Ausfallgefahr.

Beispiel für ein statifizierendes CMS

Cliparts are licenced under Creative commons

CMS in DMZ



In diesem Fall erzeugt das CMS statische Seiten. Ein Angriff aus dem Internet auf das CMS ist schon von der Netzwerktopologie her ausgeschlossen.

Fazit

Für maximale Sicherheit und maximale Performance ist eine Statifizierung der Inhalte sinnvoll.