Attacken auf Rechner unterbinden

01.07.2025 21:02:40

FAQ-Artikel-Ausdruck

Kategorie:	Mein Zugang	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	11:55:55 - 08.02.2025

Schlüsselwörter

Brute, Force, Attacke, unterbinden, sperren, Firewall ssh, vpn, server, pc, Viren, sicher, Sicherheit

Symptom (öffentlich)

Ich habe eine Attacke auf einen von mir betriebenen Rechner festgestellt.
Wie kann ich mich schützen?

Problem (öffentlich)

Ich muss Zugriff aus dem Internet auf einen Rechner haben, dazu muss ich einen Zugang (ähnlich einem Tor) öffnen.
Dann muss ich damit rechnen, dass auch unberechtigte Personen versuchen werden, diesen Zugang zu missbrauchen.

Lösung (öffentlich)

VPN nutzen Handelt es sich um den Zugang zu einem Server im Institut, kann durchaus VPN genutzt werden und jeder weitere Zugriff direkt aus dem Internet über eine Firewall geblockt werden. Passwort In jedem Fall sollten sichere Passwörter verwendet werden. Ein echtes Wort wie z. B. "Urlaub" ist definitiv kein sicheres Passwort. Es sollten Passwörter von Zugangskennungen mit entsprechenden Rechten auch regelmäßig geändert werden.
Weitere Hinweise zum Thema Passwort finden Sie unter:[1] FAQ#10001536. Erhöhte Rechte Konfiguriert werden muss ein Rechner, der "von außen" erreichbar sein soll immer so, dass der Systemverwalter (root, Administrator etc.) sich nicht einloggen kann. Unter Unix, Linux, MacOS sollte administrativ nur mit Hilfe von [2]sudo (SuperuserDo) gearbeitet werden. Unter Windows sollten Administrator-Konten nicht zur täglichen Arbeit verwandt werden. Ein Wechsel der Rechte wird durch UserAccessControl (UAC) seit Windows 7 (teilweise auch schon ab XP) möglich. Firewall Brute-Force-Attacken lassen sich temporär über Firewalls sperren.
Es gibt einige Projekte, die zeitnah Regeln für Firewalls erstellen können, die den Angriff temporär blocken. Wird mehrfach ein fehlgeschlagener Login von einer bestimmten IP Adresse festgestellt, so wird diese dann blockiert.
Schlagworte für eine Internetsuche sind z. B. ssh, iptables und brute force.

[1] https://support.rz.tu-bs.de/znuny/public.pl?Action=PublicFAQZoom;ItemID=1536;Nav=
[2] http://de.wikipedia.org/wiki/Sudo