DNS-Server mit offenem AXFR

Das AXFR-Verfahren (Zonentransfer) dient zur Synchronisation der DNS-Einträge für eine Domain zwischen den autoritativen DNS-Servern. Eine AXFR-Abfrage sollte üblicherweise nur von den jeweiligen Secondary-DNS-Servern an den Primary-DNS-Server zugelassen sein.

Bei einer Fehlkonfiguration des DNS-Servers kann eine AXFR-Abfrage jedoch von jeder beliebigen IP-Adresse im Internet aus erfolgen. Angreifer nutzen dies aus, um Informationen über die mit einer Domain verbundenen Systeme zu erlangen und darüber ggf. weitere potenzielle Angriffsziele zu identifizieren.

Weitere Informationen hierzu finden Sie unter: http://www.heise.de/security/meldung/Falsch-konfigurierte-DNS-Server-liefern-Angreifern-wertvolle-Tipps-2595206.html

CERT-Bund hat eine Liste von Domain-Namen erhalten, deren autoritative DNS-Server in Deutschland gehostet werden und die eine AXFR-Abfrage von beliebigen IP-Adressen aus zulassen.

Nachfolgend senden wir Ihnen eine Liste betroffener Domain-Namen und den zuständigen DNS-Servern in Ihrem Netzbereich.

Wir möchten Sie bitten, den Sachverhalt zu prüfen und entsprechende Maßnahmen einzuleiten bzw. Ihre Kunden zu informieren.

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/dns-server-mit-offenem-axfr/