FAQ Security - DNS

Public DNS and Security

A good working DNS is mandatory to ensure good telephony quality, especially in a hosted environment.

Via this article we want to inform you of the possible security risks when using a public DNS server.

When using a public DNS server, like Google 8.8.8.8 or 8.8.4.4 and many more, there is a big chance that a Googlebot or similar mechanism will scan the router of which the DNS enquiry came from and will report the opened ports (port forwards you may have setup). As, in this case Google wants to collect as much information about the possible website behind the router, they use this mechanism as they will have more to show in their search engine.

It was brought to our attention that there are sites (which we will not reveal in this article) that will make this information available for anyone who knows such websites. You can imagine how easy it would be for hackers to try to attack your systems, especially when they can be found so easily.

As many hack tools are on the internet, all default passwords and login names will be tried first and when they are in, they can do whatever they like with your system or worse, your customers system(s).

To narrow down the risk there are several things you can do as always:

- Never use the default login and passwords, always change them into one with a high level of security when setting up systems.
- Never use a public DNS server, only the one of your Provider, this would minimize the risk of being scanned.
- Be thoughtful of port forwards and when you do not really need them, close them or at least restrict them to the IP of the originator you want to allow the packets to be forward from.
- Use only VPN to connect remotely to any systems.
- If you need remote access to a WebGui and VPN is not available, use an SSH client with tunnel capabilities and use an extremely strong password.