

Secret Router Security Discussion in Germany

Posted on **January 26,2018** by lynx

Routers are the main component when it comes to connect sites, homes, and businesses. They often „just“ take care of the access to the Internet. The firewall comes after this access device. The German Telekom suffered an [attack on their routers on 2016](#). The [German Federal Office for Information Security](#) now tries to create a policy for securing these critical systems. In theory this should add a set of documents on how to securely operate a router for the last mile access. Information security basically runs on checklists and policies. The trouble starts with the firmware. In Germany there is a discussion about using alternative devices as access components, enabling customers and organisations to use products of their own choice. Since firmware is the worst code on this planet, changing models and code is a good idea. The [Association of German Cable Operators \(ANGA\)](#) strictly opposes changes of software on modems. The working group discussing the new policy has held meetings in Bonn, but it's complicated. Furthermore participants discuss the topic with a non-disclosure agreement.

Security and secrecy don't play well together. In this case there is the question of supporting customer-operated software on access devices, but this can be solved. All companies already use software tailored to their needs. Few applications or devices are used off-the-shelf. A lot of IT departments bring devices and other components into a given state by applying patches and changes to the configuration. Surely the access to the Internet must not remain a mystery. Protocols are documented, the technology is not based on a need-to-know basis. Why not address this weak link by giving sysadmins the tools to take care of the network boundary? Especially in times of home offices and interconnected (business) applications this link must be taken into account when designing security.

[Golem.de has an article describing the process in depth](#) (and in German).

Posted in:Internet,Security | Tagged:Infrastructure,Internet | With 0 comments