asvin

Media Information

Stuttgart 16.03.2020

Working from home - home routers jeopardize corporate IT security

Due to the COVID-19 outbreak, more and more employees are currently working from their home offices. The workflow can usually be managed well. But connecting an external computer to the corporate network creates risks for information security.
for information security. One of the biggest weak points is the router in the home office. IoT security expert Mirko Ross gives tips on what companies and employees should pay attention to now.

More and more companies are allowing their employees to work from home. This is to prevent the corona virus from spreading through the workplace and infecting many people. However, this results in considerable security risks for the company's IT: Because attackers can gain access to confidential information through vulnerabilities in the employees' home network.

The danger: home routers without the latest update

The gold standard for the connection between the company and the laptop in the home office is secure access via a VPN. But, "The VPN infrastructure of many companies is not designed for the mass of home office capacity suddenly needed," explains Mirko Ross, well-known IoT & cybersecurity expert. "Many companies are therefore advising their employees at the moment to only do 'critical', i.e. particularly sensitive work, via VPN and to do without a VPN for all other work."
In practice, therefore, employees increasingly have to work via their private Internet access at home. Many are not aware of the security risks associated with the home network. The Internet router easily becomes the most insecure point in the home office. A study published by Avast in 2018, for example, found that 60% of WLAN routers can be easily attacked. This is not surprising, as one in six Germans is overwhelmed with setting up their WLAN router, according to a 2019 survey by security firm Kapersky.

But even when working with VPN, the home router can be an entry ticket for attackers in companies. For example, if access data for setting up the VPN is sent unsecured via email and attackers can tap into this as a man-in-the-middle at the poorly secured home router.

Simple hygiene measures close security gaps

Mirko Ross therefore advises companies to require employees to first take care of the security of their router before logging into the company system: "Similar to the fight against the corona virus, this involves basic hygiene measures: analogous to washing your hands and sneezing into the crook of your arm, you must provide the router with a secure password and update the router firmware in order to ward off attacks from hackers."

The first thing to check is whether the router is equipped with an automatic firmware update function. If not, you have to download the update yourself - and take care of it regularly in the future.
The second weak point - insecure, too short or factory-set passwords - can be closed quickly: A secure password should be created from a random combination of letters, digits and special characters and be at least 16 characters long.

To make this work, Mirko Ross recommends security managers support employees by providing guide- lines and, if necessary, active assistance in securing their router. If you follow these rules, you can close a major gateway that would otherwise be wide open to attackers," he says. So this small investment definitely pays off!"

Reprint free of charge, please provide proof (print, scan) or link.

Mirko Ross is an internationally recognized activist, expert, speaker, publicist and researcher in the field of cybersecurity and the Internet of Things. He is involved in IoT security as a member of the Expert Group on Internet of Things Security of the European Cyber Security Authority ENISA. In addition, Mirko Ross is active in international research projects in the field of cybersecurity and blockchain technologies and is founder and CEO of the start-up asvin and digital worx GmbH.

Image:

Portrait Mirko Ross, CEO asvin GmbH

Contact:

seidel. agentur für kommunikation
Brunnengasse 3
73650 Winterbach (Stuttgart)
T: +49 (0)7181 / 26 29 376
E: medien@seidel-kommunikation.de