Security vulnerability in mobile networks: VPN connections via 3G/4G still secure

01/05/2015

Since late December, media reports have been circulating about a serious vulnerability in 3G/4G networks. Apparently the vulnerability can be used to intercept encryption data in 3G/UMTS networks, making it possible to read e-mails and to eavesdrop on conversations. Providers encrypt customer communications with automatically generated keys, which are exchanged between telephone exchanges and other carriers. The vulnerability appears to relate to this data exchange. The Signaling System 7 (SS7) used for this purpose is reported to be vulnerable and allows the security keys to be intercepted.

Mobile communications based on VPN connections are not affected by this vulnerability: Sites networked via 3G/4G using VPN are still secure.

For VPN connections, an end-to end encryption is set up between the VPN router or VPN client at the one site and the VPN gateway at the other site. These keys are negotiated directly between the customers' VPN devices and are unknown to the network operators. For this reason, they cannot be passed on. The entire VPN communication over the cellular network is encrypted and can only be decrypted again at the end point of communication in the customer network.