Step by step towards greater network security

What you can do now to improve network security

No industry or size of company is safe from cyberattack. In what is otherwise a positive increase in the digitalization of work processes, the issue of network security becomes an even greater challenge. Read on to learn how you can immediately improve your armory against hacker attacks with the resources available to you right now:

Router and firewall settings that increase your network security

- ☐ Allow only encrypted Internet protocols like HTTPS or SSH and deactivate unnecessary or unencrypted Internet protocols like HTTP or telnet
- ☐ Block any external access to your devices and always use a VPN connection, even when configuring remote routers/firewalls
- ☐ Close unused ports in the router/firewall
- ☐ Block all Internet-based access to any end devices that are directly connected to the router (e.g. printer) and close insecure entry points
- ☐ Follow the latest security recommendations and use IKEv2 as the VPN protocol with at least AES-GCM and SHA-256 for encryption (now out of date and therefore insecure: Protocols like PPTP or algorithms like MD-5 or SHA-1)

How switches secure your network

- ☐ Deactivate any unencrypted and unused Ethernet ports
- ☐ Use VLANs to segment networks for different applications or departments: Use different VLANs to keep any configuration ports in the management VLAN isolated from the end-user networks and endpoints

- [ ] Check Ethernet-port endpoint connections and close any open ports
- [ ] Introduce port authentication via IEEE 802.1X certificates or MAC-address authentication to monitor and control port usage
- [ ] Switch off unnecessary and insecure remote configuration channels

How access points help to secure company networks

- [ ] Use the latest encryption standard WPA3
- [ ] Reduce the transmission power of the access points to a minimum:
  Prevent your network from being received outside your own premises
- [ ] Separate the Wi-Fi into different SSIDs for specific user groups
- [ ] PPSK / LEPS: Private pre-shared keys (PPSK) for users or LEPS with LANCOM devices allow you to restrict and better monitor endpoint authorizations or to remove individual employee keys from the database when they leave the company

Help you personnel to have better general awareness of IT security at work

- [ ] Offer regular training courses for employees, e.g. on secure passwords or how to deal with phishing mails
- [ ] Prevent the use of unauthorized USB sticks and other private data media from connecting to the company network
- [ ] Keep everything up to date and regularly install the latest security updates for software and device
- [ ] Organize daily data backups
- [ ] Use a customized, professional UTM (Unified Threat Management) firewall
- [ ] Work with IT administrators and specialist resellers to develop an overall cybersecurity concept and eliminate any vulnerabilities found