

Cyber Security Solutions

for BARTEC BENKE Analyzers



Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks, also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and it can be divided into a few common categories. The most important parts are network security, application security, information security and end-user education. In a more and more connected world with always new upcoming threats, it is very important to establish measures against these threats.

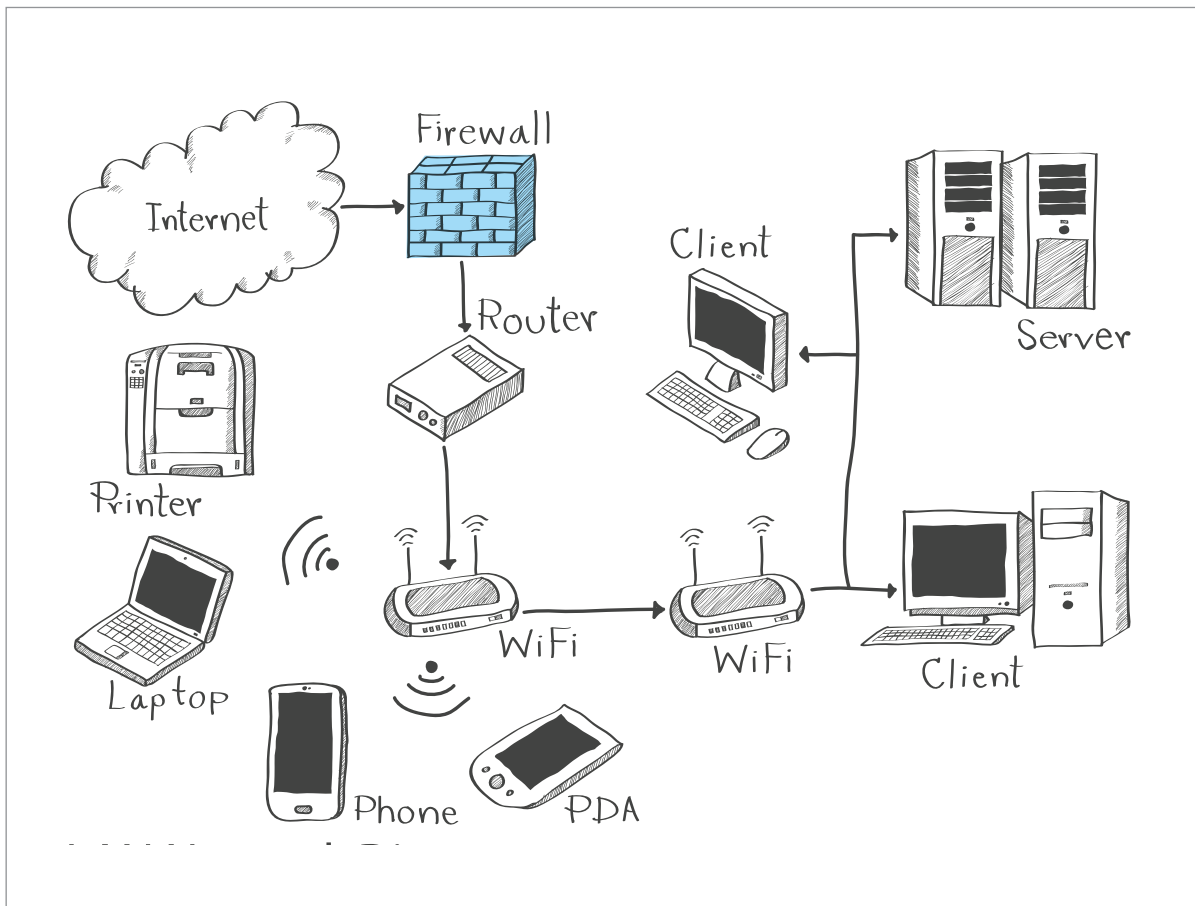
Threats can vary and have a diversity of consequences. Here are some examples:

- hacker will use malicious software to close computer systems or to code them and blackmail users for money to handover data
- many injured employees
- evacuated residents
- airlines need extremely cost-intensive stopovers of their long-haul flights due to lack of fuel
- for oil markets, any pipeline stop/cancellation will produce increasing prices
- refinery operational capacities decrease significantly
- pollution through oil tanker accidents or offshore platforms

With cyber attacks, PC working places are affected for weeks and cause industrial accidents. Additionally:

- computers need to be re-set up
- infected manufacturing machines have to get replaced
- new network servers have to be bought
- the operational failure causes more costs for IT experts, new hardware and through spam-eMails it causes an image damage

That is why BARTEC created a policy of company site regulations that defines our environment and shows how we need to protect it. Being a customer, you will always get a system with a fundamental level of security. This means that we guarantee a system that is proven free of malicious data and has enabled mechanisms for protection against external threats. We only deliver this level until commission because we cannot guarantee for the secureness within customer networks.



Real case approach

BARTEC BENKE has regular contact with its customers in order to keep the analyzer and systems updated. Upgrades for cyber security become more and more important. Here are the process steps how BARTEC BENKE analyses specific needs of the customer:

- As a part of the worldwide BARTEC Group, we are following the “Corporate IT”-guidelines.
- BARTEC IT equipment itself is selected in terms of security and availability by the global IT department. All BARTEC companies can order only selected equipment.
- BARTEC IT systems and applications may only be used for company purposes.
- Deployed IT equipment is prevented against mal-operation and irregularities to the greatest extent possible to guarantee data completeness, integrity and accountability. Globally used IT systems of the group such as ERP, CRM, Email-system and virus-protection are configured, managed and maintained by the IT administrators of the BARTEC group.
- The password quality of passwords within the BARTEC BENKE company is required by the BARTEC group.
- The site location BARTEC BENKE in Reinbek has several measures to comply the global regulations.

- age of analyzer at customers location
- can we keep the analyzer or do we need to replace it
- what would the analyzer need in terms of Windows upgrades
- would this include new hardware such as new PC and maybe new IO card etc.
- a technical summary will conclude the final needs of the customer
- BARTEC BENKE would develop a RFQ for customer for further action

The cyber security plan

The cyber security plan is specified on our physical property analyzer systems. BARTEC BENKE analyzers are always constructed according to the same principle. Therefore we can define general methods and procedures to secure an analyzer properly.

We guarantee a fundamental level of security at all analyzing systems. The following list will show the measures and tests that will be performed. These definitions are only valid for a physical property analyzer with the operating system Windows 10 embedded.

PERFORMED ACTIONS PRIOR TO COMMISSION AS STANDARD:

- Anti-virus-software* is installed and activated
- Windows is up to date
- Standard windows firewall is active
- Daily PACS backup
- Full virus-scan
- Real-Time Protection of system
- Documentation of all created user accounts, installed programs and firewall-rules
- Execution and documentation of well-established cyber-security tests**
- Documentation and verification of all performed actions, including software versions

OPTIONALLY PERFORMED ACTIONS PRIOR TO COMMISSION:

- Hardware locks for interfaces
- Second user account for normal operation without admin access
- Static IP-address

OPTIONAL REPEATING SECURITY CHECKS:

- Check of performed and recorded actions
- Update of system, if possible
- Perform actions to close security gaps, if necessary

* All analyzers are supplied with the anti-virus software Microsoft Windows Defender. Latest findings (e.g. ct magazine, issue 3/2019) indicate that Microsoft Windows Defender is fully sufficient to provide comprehensive protection against viruses.

** We use OpenVAS (Open Vulnerability Assessment Scanner, recommended by the BSI - Federal Office for Information Security) to scan and test the analyzer system.



BARTEC BENKE has also developed the **OSM – Operating System Maintenance Manual**, which describes the handling of updates, virus software, backups, user accounts and remote access to make sure that the operating system of the Analyzer Control Unit (ACU) is working securely and trouble-free. Here you can find recommendations and tips as a user. Based on that, you will maintain the highest level of security, which you can achieve for your operations.

Included in our “Cyber-Security-Plan”, we will guarantee a secure and virus-free system at commission. This statement is valid for all physical property analyzer from BARTEC BENKE GmbH.

We are offering an additional option called “Cyber-Security-Package”. This package includes an examination at every service job regarding our cyber-security-concept. This test is based on the initial operation examination and will check the system on threats, changes and basic security based on our hardening guide and additional agreed options.

Contact us for more information!

BARTEC BENKE GmbH

Borsigstr. 10
21465 Reinbek/Hamburg
Germany

Tel.: +49 40 72703 0
sales-reinbek@bartec.com

bartec.com