IT security / cyber security at W&T

As a company, we have been involved in connecting and networking systems since our beginnings in the late 1970s. Our wealth of experience has grown accordingly over the years. Unfortunately, where there is light, there is also shadow, which is why the topic of IT security has been with us for a long time. We not only take care of our own security with the care you are familiar with, but also consider this aspect when developing our devices.

We monitor current developments in the threat situation and legislative processes very closely. We are happy to provide information on the following key points:

Information security management / ISO 27001

Our information security management is not (yet) certified. We have so far dispensed with this formality, but we understand the need of customers to obtain information easily via neutral third parties, which is why a certification process is currently being considered.

Our internal network is deeply segregated, in particular the production area is completely encapsulated and separated from the administration and development area, for example. Our systems and applications are hardened and secured, firewalls and virus protection are active and systematic update and patch management is in place.

Our in-depth backup management puts us in a position to be operational again with only minor data loss in the event of an incident.

We will of course inform you in the event of an incident. We will continue to monitor all NIS-2 related developments, even if we do not currently appear to be directly affected due to the size of our company.

Cyber security at product level

Our devices (and their firmware) have historically been designed for quick and easy commissioning (and use) and therefore often do not have a default password, for example.

Nevertheless, all devices have extensive hardening options that can be used or “enforced” during commissioning. Please also refer to the relevant product documentation / instructions. Please also contact us for individual standard configurations and hardening measures.

W&T has always been known for fast and constructive support. This also applies to cyber security: we have an established internal vulnerability management system and offer updates and fixes within a very short time if the worst comes to the worst. We also work together with Cert@VDE and engage in a professional exchange.

As a component manufacturer, we naturally follow the processes surrounding the Cyber Resilience Act at a formal level and also examine certification options here.

Wiesemann & Theis GmbH
Porschestr. 12
42279 Wuppertal | Germany
GF: Tobias Theis (M.Eng.)

Tel.: +49 202 2680-0
Fax: +49 202 2680-265
info@wut.de
www.wut.de

Handelsregister:
Amtsgericht Wuppertal
HRB6377
USt-ID: DE121008340

All questions about cyber security or vulnerabilities in W&T devices can be addressed explicitly to security@wut.de in addition to the usual channels.

Wuppertal, 15.07.2024

Tobias Theis (M.Eng.), General Manager

Wiesemann & Theis GmbH
Porschestr. 12
42279 Wuppertal | Germany
GF: Tobias Theis (M.Eng.)

Tel.: +49 202 2680-0
Fax: +49 202 2680-265
info@wut.de
www.wut.de

Handelsregister:
Amtsgericht Wuppertal
HRB6377
USt-ID: DE121008340