



## Logging and monitoring

### A further step towards improved security

As stipulated in white papers published by the Federal Association of Energy and Water Industries and as a consequence of certification in accordance with ISO/IEC 27001, **operators of critical infrastructure** have to **better protect and control** their systems and devices. This is why we offer two new services to our customers – device logging and system monitoring.

Both services are **not restricted** to your grid control systems, but can be applied to your **whole IT infrastructure**. By means of logging and monitoring, you are able to analyse anomalies and attacks. Our two new services are important tools to **detect security holes** and thus help you in **facing future challenges** successfully.

#### What is logging?

Almost every device within a network stores various information into log files. These files, however, are limited in size and often only available for a couple of seconds.

Typically logged details are:

- logins/logouts, login attempts
- changes to the configuration
- failed attempts to access the system
- VPN connections
- error messages

Logging systems can **store such device information centrally for a longer time** and you are thus able to **evaluate it later**. Not only white papers published by the Federal Association of Energy and Water Industries but also the standard ISO/IEC 27001 demand for logging as security measure.

Thanks to the aforementioned details you are better prepared for future attacks.

#### What is monitoring?

A monitoring tool permanently surveys specific system parameters and is thus able to detect when these parameters differ from standards or defaults.

Typical parameters are:

- CPU temperature
- CPU load
- hard disc capacity/hard disc errors
- active operating times
- availability of services

The monitoring tool continuously observes your systems, verifies proper function and **triggers alarms in case of disturbances**. Monitoring is also mentioned in ISO/IEC 27001.

The details mentioned above improve the knowledge about your system and enable further optimization.

✓ Little effort for great benefit

✓ Proof of security in compliance with German regulations  
and ISO/IEC 27001

✓ Verification of availability and stability of your information technology

✓ Early recognition of critical operating conditions



### Logging This is our offer

For logging, we count on  
ProLog by NETZWERK Software GmbH.

#### Step 1: software

We provide you with the required  
software licence.

#### Step 2: preparation and specification

Together we define devices and events to be  
monitored, retention times and access rights  
as well as data transfer to the logging server.  
Based on these demands, we develop a  
logging concept.

#### Step 3: commissioning

We provide commissioning in a virtual  
environment, registration, firewall configuration  
and instruction of users.

If required, we can also offer time or  
event-oriented evaluations as a service.

Please contact us!



### Monitoring This is our offer

For monitoring, we count on  
PRTG Network Monitor by Paessler AG.

#### Step 1: software

We provide you with the required  
software licence.

#### Step 2: preparation and specification

Together we define devices and events to  
be monitored, alarms in case of disturbances  
as well as data transfer.

#### Step 3: commissioning

We provide commissioning on an independent  
Microsoft Windows server, registration,  
server configuration, domain controller and  
workstations as well as instruction of users.

If required, we can also offer time or  
event-oriented adaptations of evaluation and  
alarms as a service.

Please contact us!