



## RECOMMENDATION: IT IN PRODUCTION

# Case example remote monitoring

## Whom has my mobile radio modem called?

The BSI received information regarding the misuse of mobile radio modems.

### 1 What happened?

The cases which became known to the BSI were about mobile radio modems used for system monitoring. They were misused for DoS attacks and resulted in large mobile phone bills. Devices of this type are not only connected to the Internet, but also to the telephone network. This was detected only after several months and already paid bills.

### 2 What do mobile radio modems do?

Mobile radio modems use the transmission channels of mobile phone networks and are used for remote control purposes of all kinds. Data is transmitted comparably to smartphones. In addition to simple data transmission, mobile radio modems also allow sending SMS, voice messages and fax via the telephony service functions, for example for status and alerting messages. Some of these functions, however, can also be misused; examples of this include dialling value-added services or sending SPAM SMS. Via the mobile phone network, the devices themselves provide access to the Internet where they are subject to additional threats. On the one hand, attacks and misuse by these means can be designed in such a way that operations are limited or even become impossible and, on the other hand, that they neither interfere with nor affect the actual application purpose in any other way.

### 3 What was the reason for this?

When performing analyses, it was determined that modems were configured inappropriately. For example, default passwords were not changed. Thus, attackers were able to gain access. Afterwards, the network connections and the integrated functions were misused to use the systems as part of a DoS attack. This resulted in a higher data volume and, as a consequence, in significant additional costs for the operator. Another possibility for the perpetrator could also have been to manipulate the devices, for example to send spam mails. Furthermore, only random checks of the bills caused that the higher amounts and thus the misuse remained undetected for a longer period of time.

## 4 Lessons learned

As a matter of principle, components which can be accessed from the Internet must be configured securely. This includes in particular that access data available by default is exchanged and the components are supplied with security updates as quickly as possible.

In addition to these basic requirements, the attack could have been detected quickly and additional costs avoided by regular checks of the data volume or by a warning when threshold values have been exceeded. For this purpose, monitoring can be set to trigger messages at an early stage when unusual or undesirable states occur. Monitoring can be implemented by the following safeguards:

- Logging of the data volume and, related to this,
  - Monitoring of services used by default and
  - Registration and notification of lower deviations or exceedance of prescribed threshold values in the data volume.
- Checking the bills and itemised bills for abnormalities:
  - above-average or occasionally higher invoice amounts by a higher data volume, telephone connections subject to a charge, such as value-added services and/or SMS dispatch
  - Connections to unknown or unusual targets

Further safeguards also include suitable archiving for subsequent analysis and, where necessary, tools for automated examination and evaluation.

## 5 Summary

In addition to the basic requirements for the protection of systems, monitoring is a module in being able to identify and respond to attacks. This increases the security and also allows the assessment of the availability and the identification of a possible need for optimisation. This does not only apply to the mobile radio modem in this sample case. Monitoring is recommended in all network applications, especially in industrial control systems and critical environments.

## 6 Additional information

Among other things, the document "Top 10 ICS Threats and Countermeasures" is recommended as further literature for the cyber security threats of industrial systems. The ICS Security Compendium of the BSI is suitable as a basis for the protection of control systems and industrial systems. These and further documents are available at:

[ICS Security Compendium \(https://www.bsi.bund.de/ICS-Security-Kompendium\)](https://www.bsi.bund.de/ICS-Security-Kompendium)

By means of the BSI publications, the Federal Office for Information Security (BSI) publishes documents about current topics in the field of cyber security. Comments and advice from readers can be sent to [info@cyber-allianz.de](mailto:info@cyber-allianz.de).