German
Business Protection

**Risk Consultancy**
**Business Enablement**
**Compliance & Security**

# Security Threats Germany

## October 2016

**Berlin, October 12th 2016**


| | |
|---|---|
| Hotline | +49 30 63967027-0 |
| Fax | +49 30 63967027-99 |
| E-Mail | info@gbp-security.com |
| Internet | gbp-security.com |

## Information Protection and Electronic Cameras

According to research by the ARD magazine FAKT, a surveillance system manufacturer have built in secret access for US secret services in their products. The situation involves the American firm NetBotz, who were taken over by the French corporation Schneider Electric in 2007. The surveillance systems sold by NetBotz have been mainly installed in security areas such as server rooms, i.e. in places where system administrators work.

According to FAKT, the Bundesnachrichtendienst (BND, or Federal Intelligence Service) have been aware of this fact since 2005; however, this information was not relayed to the Bundesamt für Verfassungsschutz (BfV, or Federal Intelligence Service Agency) who only learned about it in 2015 through an investigation of the event by the Bundesanwaltschaft (Federal Prosecutor's Office). NetBotz have publicly endeavoured to acquire clients in the high-tech and industry sectors since 2005, and surveillance systems were underpriced, partly as a means of obtaining orders.

Moreover, NetBotz's approach does not appear to be a one-off incident. In the United Kingdom, the 'motherland' of surveillance systems, it recently came to light that the Chinese firm Hikvision have sold over a million cameras to its clients, all of which are web-enabled. The surveillance systems in this instance were also installed in sensitive areas, such as airports. These systems can recognise and track people as well as number plates. Hikvision are under the control of the Chinese state and have close ties to security authorities which, from our perspective, are dangerous ties.

As well as camera solutions which are used in the commercial sector, and which can potentially provide gaps in security, private households can also attract the attention of hackers through the use of WiFi-enabled video cameras in home networks. If such cameras are connected to a router and / or a home / firm network, there is a danger that this network, be it private or corporate, is vulnerable to attacks. Amongst other things, hackers are able to turn off the firewall or even read, destroy or change any and all information. This vulnerability is a result of many cameras not using password protection, which really should be standard practice for such devices in this day and age.

If a surveillance camera or a webcam becomes an unwanted spy, rather than serving its intended functions of surveillance and subsequently protecting important information for the firm, this can be a dream scenario for burglars, cyber criminals or security services. Even if these devices are protected by passwords, private users in particular often do not change preset passwords or passwords supplied by the manufacturer's website, which makes it easy for potential hackers to exploit these gaps for criminal purposes. Anything associated with the network can be hacked, especially when users make this kind of intrusion easier. Firms should therefore consider not building web-enabled surveillance equipment in sensitive areas. In other instances, users are well advised to use strong passwords and avoid devices which do not provide any adequate security settings.