German
Business Protection

Risk Consultancy
Business Enablement
Health & Safety
Compliance & Security

Security Threats Germany

August 2017

Berlin, August 16th 2017

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

The German redefinition of IT monitoring

The Federal Criminal Police Office (BKA) is equipping its IT. Already this year, the BKA wants to use a so-called "state trojan" in order to hack smartphones and read encrypted messages. This development is due to a decision of the Bundestag, which allows the security authorities henceforth with appropriate judicial permission to inject monitoring software on PCs or smartphones of potential criminal suspects. Until now, the BKA was only allowed to hack devices when it came to the prevention of international terrorism.

The BKA itself programmed the Trojan: the so-called "Remote Communication Interception Software" (RCIS), which was used for the first time in 2016. In addition to self-developed Trojans, the BKA also uses commercial monitoring software. This software was developed by an external company and is to serve as a replacement Trojan, in case RCIS is detected. However, fact is that this "external" tool can do a lot more than RCIS and the manufacturer advertises it as a complete portfolio of hacking tools.

The decision of the Bundestag to massively expand the use of Trojans in order to strengthen the fight against organized crime and terrorism is to be welcomed. However, one must bear in mind that not only German authorities use such tools to get sensitive data.

Although the external partner of the BKA officially excludes the sale of its surveillance software to totalitarian regimes, the Wall Street Journal has already published a secret memo of the Egyptian Ministry of the Interior in 2011, which shows that the software was also offered to the authorities in Cairo. It is therefore to be assumed that both foreign services and criminal groups have been given access to this technology and that they are thus able to pursue economic espionage.

For companies this has a very clear consequence - no electronic exchange is absolutely secure. One must expect that everything can be intercepted. Only one can no longer know what was caught and by whom - was it the BKA or a third party? Highly sensitive information and business secrets should therefore be transported in a classical manner: Through the errand to the business partner. Otherwise it could be the revival of the old mechanical typewriter...