German
Business Protection

Risk Consultancy
Business Enablement
Compliance & Security

Security Threats Germany

September 2016

Berlin, August 26th 2016

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

Attacks on Industrial Control Systems on the increase

Companies and utilities use Industrial Control Systems (ICS) in order to manage processes such as power generation, water management or automated manufacturing. Last year the US Department of Homeland Security (DHS) reported 295 cyber-attacks on factories and utilities. Security experts suspect that foreign Security Services and Organized Crime groups are behind these worrying attacks on the critical infrastructure of the United States. Furthermore, experts believe, that the black – out in the Ukraine at the end of last year were the result of a targeted attack.

During the course of a penetration test in Germany early this year experts were able to access the control systems of a waterworks via the internet. By acquiring the administration rights, the experts would have been able to take control of the water pumps and would thus have been able to cut the water supply.

In April of this year, a computer virus was found in the control system of the German nuclear power plant in Grundremmingen. The installed software would have enabled a direct connection to the Internet and thus the possibility of taking over control of the power station. The management of the plant stated that the population was at no time at risk, however it is important to remember that access via internet is the preferred route for hackers.

The rise of private companies developing software and tools which have enabled hackers to access data and systems is also worrying. The Italian company Hacking Team or Washington based Zerodium sell to authorities, but since an attack on Hacking Team in July 2015 much of the know – how and programs have been posted and used by cyber gangs.

In August of this year the news reached us, that the most powerful spy agency in the world, the NSA, had become a victim of a cyber-attack. As in the case of Hacking Team a number of details were published on the internet, other files were encrypted and the key sold to the highest bidder.

A parallel development is the rapid rise of software providers offering either services or software via the DarkWeb. Criminal users of such software are thus increasingly able to access systems and hold the users to ransom. If a certain sum is not payed (in Bitcoins), the criminals threaten to erase or corrupt files causing massive potential damage.

In the light of these worrying developments it is now understandable, why the German authorities are urging organisations to tighten up defenses and security protocols. The authorities are also suggesting that private households lay in supplies for up to 15 days. Given the potential disruption a cyber - attack could have on the critical infrastructure of the country these steps are more than sensible.