Cyber Security Summit 2014 – Documentation of the working groups

Working Group 4: How To Prevent A Digital Emergency?

Sneaking in through the back door

When professional cyber criminals go to work, they first try to illuminate the environments in which their intended victims operate. That can lead to "open Sesame", firewalls and virus scanners notwithstanding. Rik Ferguson,Vice President Security Research at Trend Micro, and Holger Junker, head of the BSI's (Federal Office for Information Security) ICS Security Unit, showed how easy it can be to hack smartphones and machines.

229 days. More than 7 months. That's how long it now takes, on average, for companies to detect cyber attacks against their IT systems. Attackers hold all the trumps. With their time advantage, they have all the time in the world to steal the data their customers are looking for. "The existing modes of defense simply don't work anymore," explains Rik Ferguson. "Attackers simply fly under the radar." The primary goal should thus no longer be to block hackers. Instead, he explained, companies need to identify their weaknesses and find out who has already penetrated into their systems. "Then, they can keep attackers from leaving with business-critical information," Ferguson explains.

"Mobile devices are the easiest devices to hack. And they have lifted the natural boundaries of companies," explained Ferguson in Bonn. Then, with a live hack, he gave an impressive demonstration of how vulnerable smartphones are. He placed an invisible app on his victim's device and used his own smartphone to text commands to the program. With such commands, for example, one can have the app record conversations and transfer them to a website for download. Or have the app switch the device's microphone on, to enable the attacker to listen in on an important meeting. The espionage app leaves no traces whatsoever on the victim's smartphone. The text traffic remains hidden, and the app can be deleted remotely at any time.

Risks for industry 4.0

Increasingly, machines are also coming under threat from hackers, as sabotage viruses such as Stuxnet and Havex show. "Machines today have industrial Internet communications links and thus can basically be hacked. We have seen a massive jump in attacks against industrial control systems (ICS)," explained Holger Junker, ICS-security expert with the Federal Office for Information Security (BSI). For example, hackers spread their malware via "watering hole attacks." In such attacks, they might use an ICS manufacturer's website to infect software that users can download online. That can enable a malware program to spread very quickly. Today's antivirus programs do not protect against malware for ICS, Junker warned. For this reason, new security solutions need to be developed for industry 4.0. With a mini robot, he demonstrated how easy it is to manipulate machines.

In closing, BSI President Michael Hange discussed the three critical weaknesses of current systems. Software itself contains an average of five errors, and thus five weaknesses, per thousand lines of program code, he noted. The "always on" mentality, and the ubiquitous availability of systems as a result of use of mobile devices, make it much more difficult to defend against attacks, he explained. Finally, hacking is now a highly lucrative business that has very small risks, he pointed out. In Hange's view, the only way to provide lasting protection is to rely heavily on cryptography. And yet use of encryption is still very uncommon, he said.