Cyber Security Summit 2014 – documentation

Keynote Ashar Aziz, Founder and Vice Chairman of the Board FireEye

Cyber crime compromises shareholder value

From a youthful experiment to the biggest threat of the 21st century – Ashar Aziz, founder and Vice Chairman of the Board of the U.S. cyber security provider FireEye, gave an overview of the historical development of malware and the current threat situation.

"Every software has weaknesses," stated the founder and Vice Chairman of the Board of FireEye, a U.S. security solutions provider the leader in stopping today's advanced cyber attacks. Finding and exploiting these weaknesses has been at the heart of cyber crime since the year one. Starting one day in 1981, when a young guy with too much time on his hands developed the first self-replicating program in the world, Aziz outlined the development of malware.

Within this process, the development of increasingly sophisticated IT systems brought with it ever-stronger parallels with the real world. Alongside spies we now have cyber spies, while alongside terrorists we have cyber terrorists. Cyber crime is as difficult to eradicate as crime in the non-digital world. Current threats are not limited to specific regions of the world. Wherever there are digital networks, there are weaknesses, he said.

Undetected attacks a problem for SMEs

A fundamental problem facing today's security landscape, according to Aziz, are outdated security models that fail to recognize a whole range of attacks. This means that a small or medium-sized enterprises takes anon average take of 229 days simply to detect that an attack has taken place. In 67 percent of cases, the companies affected first hear of the incident from a third party.

Aziz then outlined the individual steps of an attack, from the infiltration of the network up to the theft of data. Following his report on cyber attacks in recent years, such as "Operation Aurora" in 2009 that led to massive attacks from China on companies such as Google, he listed current targets of attacks. Alongside government networks, energy suppliers, telecommunications providers and financial services providers are apparently top targets, in Germany as well as elsewhere. An awareness of cyber security does seem to have reached top management level around the world, however; at the end of the day, attacks have a negative effect on shareholder value. Attacks need to be detected sooner if the situation is to be improved, something that will only be possible if the defense infrastructure is expanded, said Aziz.