3 QUESTIONS FOR... JENS-PHILIPP JUNG, CEO OF LINK11

1. Mr. Jung, DDoS attacks are among the oldest forms of cybercrime. How dangerous is this form of attack at the present time?

Criminals have been using Distributed Denial of Service (DDoS) attacks to close down systems for more than 15 years. But whereas earlier attacks mainly targeted gaming servers or e-commerce websites, nowadays they are aimed at all sectors of business and industry and every size of company or organization. And the number of attacks is growing alarmingly. Every day, the Link11 Security Operation Center (LSOC) registers over 100 attacks of this kind on targets in Germany, Austria and Switzerland. When tracking these attacks, LSOC is increasingly measuring peak bandwidths well in excess of 50-60 Gbps, with some higher than 100 Gbps.

What's more, the attackers are extremely resourceful in creating new infrastructures for the launching of DDoS attacks. They have access to an ICT infrastructure with increasing bandwidth and a growing number of internet-capable devices such as home routers, smartphones and cloud servers rented with false credit card information. In our view, DDoS attacks are becoming even more dangerous.

2. What damage can successful DDoS attacks cause?

Every day companies, websites and public institutions have problems with the availability and performance of their infrastructures as a result of DDoS attacks. The downtimes for these systems, which have little or only inadequate protection, can amount to several days. During the past few months there have been successful attacks in Germany on the iPad POS system orderbird, hosting providers Strato and Uberspace, remote PC support specialist Teamviewer, and the websites of the major German cinema chains.

The case of Swiss company Digitec has demonstrated clearly that the consequences of DDoS attacks can extend far beyond the website. The prolonged and recurring attacks against the online home electronics retailer in mid-March 2016 shut down both the online shop and the enterprise resource planning (ERP) system, with the result that the sales outlets and the call center which deals with customer service were also put out of action. Despite incidents such as this, all too few companies are taking precautions to protect themselves.

3. How can companies protect themselves against these attacks?

There are many different types of DDoS attacks. A simple attack can be warded off completely with little difficulty. On the other hand, there are new forms of attack on companies' network infrastructures. According to our analyses, these are increasingly complex attacks which exploit security gaps using special malware. Other attackers try to gain access by way of a very large bandwidth (more than 100 Gbps). Practical experience has shown that most firms are unable to counter the growing DDoS threat effectively with their current IT security systems. To solve this problem and keep pace

with the attackers, a high level of financial and human resources is required, backed up by daily training.

The most reliable means of safeguarding companies against DDoS attacks is therefore to redirect data traffic via an external security provider. This type of professional DDoS protection has a highly developed filter center with specialists working 24/7 and with all the necessary resources to filter out unwanted data flows.