ALL WEBSITES, BLOGS AND ONLINE SHOPS are vulnerable. Hackers bombard web servers with requests for information, until the site is paralyzed. And the process is faster and more potent if the requests come from computers scattered around the globe. Even the best firewalls stand little chance against this type of DDoS assault.

HIGH SUCCESS RATE, LOW PRICES
According to the German Federal Office for Information Security (BSI), the number of DDoS incidents recorded in 2013 was significantly higher than in the previous year. And as IT security analysts at Pierre Audoin Consultants (PAC) reveal, there are 1.4 successful attacks on average per enterprise, per week worldwide. The resulting downtime causes economic damage equivalent to an average of 7.2 million US dollars per year and company. “And we only expect the number of DDoS attacks to continue rising,” remarks BSI President Michael Hange. This can be traced back to the high success rate of this form of cybercrime, not to mention the fact that hackers can be booked for a relatively low price. Their services start at as little as a few hundred euros.

“Because producing identity documents involves sensitive, personal data, we’ve always protected our systems with a variety of security solutions,” emphasizes Holger Rieger, Head of IT Security at the Federal Printing Office. These include firewalls, tunneled connections, and cryptography. Since the introduction of the e-passport in 2005 and new machine-readable German ID cards in 2010, the application process has been digitized – making it vital for the office to be online at all times. “Where required, we can issue passports within 48 hours – but only if we have 24/7 availability. As we look to expand our portfolio of full ID management solutions and products, this will only become more important,” explains Rieger.

FIREWALLS FALL SHORT
The need to guarantee around-the-clock availability, and the increasing likelihood of a DDoS strike, led the Federal Printing Office to beef up their online security. “Combatting DDoS attacks is particularly challenging – the firewall recognizes the infiltration, but its only option is to shut everything off. It cuts all Internet connections and the web servers go down,” explains Jürgen Schoolmann, Director of IT at the Federal Printing Office. “This protects the website, but it doesn’t really help us. It severely restricts our work for hours on end, or, in the worst-case scenario, even days.”

DDoS hackers have a variety of motives: blackmail, revenge for perceived wrongs, and attempts to undermine the competition can all be on the agenda. And these criminals will stop at nothing – not even at NATO. An attack in late March 2014 took several of the organization’s sites offline for a number of hours. The Ukrainian hacker group Cyber Berkut claimed responsibility. Their goal? To get “NATO cyber bandits to leave Ukraine immediately”.

At the same time, gaming giant Blizzard was struggling with a huge wave of attacks on its servers, resulting in disruptions to play and angry online gamers across the globe. Community Manager Nidorian issued an apology, explaining, “Over the course of the last week, Diablo III, World of Warcraft, StarCraft II, and Hearthstone players may have been impacted by high latency and disconnections during their gaming experience that are the result of a series of DDoS attacks on certain European Internet service providers.”

But what if all systems are go and attacks are still getting through? “We needed a way of stopping potential threats before they even reached the firewall. So the next logical step was to go to our Internet provider – T-Systems,” explains Schoolmann. Deutsche Telekom operates its own dedicated Cyber Defense Center. Its tasks include monitoring all data traffic on the backbone network – in order to recognize and respond to dangers before they reach customers’ firewalls.

T-Systems now examines all network traffic to the Federal Printing Office, checking for anomalies and filtering out any suspect data streams before they can cause a problem. Holger Rieger compares their service to a tsunami warning – only he says it’s even better: “It’s not just that T-Systems knows a monster wave is about to hit the coast and warns us – they can actually..."
stop the wave altogether or at least reduce its impact." This kind of service is not available off the peg: an extensive analysis of "normal" network traffic is essential. Rieger continues: "A regular flood is nothing like a tsunami – but the flood looks different for each company." The Federal Printing Office, for example, tends to experience the highest volume of traffic when local government offices for address registration and passport applications are open. And the data comes from German servers – whereas DDoS attacks make use of computers around the world.

**IT SECURITY AS A SERVICE**

The Federal Printing Office might look for external support when it comes to fending off DDoS attacks, but entering into a full outsourcing agreement remains out of the question for Jürgen Schoolmann. "It's important for companies to work out their own IT security management process, and then they can add the specific services they require."

As Ovum analyst Andrew Kellett notes, managed services are particularly effective when they improve on conventional security systems. He outlines: "Security risks are continuously evolving, and at a rapid pace, too. This makes it extremely difficult – or even impossible – for most organizations to keep up. Companies benefit from being part of a community that discovers and exchanges information on new dangers early. They can then deal with the problem before it can develop into a serious threat."