corero
FIRST LINE OF DEFENSE

SUMMARY

INDUSTRY
Powerful regional carrier with additional range of added value and network services

CHALLENGE
Automated defense against modern DDoS attacks to prevent server failures and focus 100% on core business again

SOLUTION
Corero SmartWall® Threat Defense System (TDS)

RESULTS
> Normal operation can be maintained 100% at all times without influencing existing systems or having to constantly implement changes.

> htp offers a solution for securing all transit connections and conveniently protecting underlying infrastructure.

> Effective protection against modern DDoS attacks using the in-line method with no viable alternative for htp; detection of DDoS attacks before they reach a critical threshold level.

MAIN BENEFITS
> Automated solution allows htp to focus on core business rather than defending against DDoS attacks using free resources.

> Effective protection against application layer and multi-vector attacks, even those that last less than 5 minutes and require only minimal bandwidth.

> Additional service that the carrier can offer to customers who are taking providers up on their promise of providing defense against DDoS attacks to an increasing extent.

htp GmbH IN HANOVER PLACES ITS TRUST IN DDOS PROTECTION PROVIDED BY CORERO NETWORK SECURITY

THE CUSTOMER

htp was founded in Hanover in 1996 and has since become one of the largest regional carriers in Germany with more than 200 employees. The company focuses on offering high-quality products at competitive prices. One specific advantage for customers is that all departments responsible for making decisions at htp are based in Hanover and are therefore easy to reach directly whenever necessary. The organizations behind htp are Stadtwerke Hannover AG, which is a 50 % shareholder, and EWE AG based in Oldenburg, which also has a 50 % share of the company.

The company product range includes telephone and DSL connections with different bandwidths, mobile communications offers and a range of network services as well as scalable data and infrastructure solutions offered by high-availability and high-security in-house computer centers. htp serves more than 9,600 business customers and approximately 88,800 private customers in the Hanover region, Brunswick and the districts of Hildesheim, Peine and Wolfenbüttel.

THE EVOLUTION OF DDOS ATTACKS AND THE CONSEQUENCES FOR INTERNET SERVICE PROVIDERS

The World Wide Web has gone through countless changes over the last 25 years, and that includes various attempts to manipulate it. DDoS attacks are just one example of such attempts, which have evolved from purely volumetric attacks to sophisticated, low-bandwidth attacks. The vast majority of current attacks have almost nothing in common with the traditional volumetric attacks, as “new” attacks are not only more sophisticated and deceptive, they occur more frequently. Traditional countermeasures are no longer able to defeat these attacks effectively, which poses a great risk for ISPs and carriers.

More recently, DDoS attacks have once again taken on a different form in all areas: volume, sophistication, and frequency. At the same time, carrier and ISP networks have also evolved and grown immensely over time.

This large amount of aggregated bandwidth further allows DDoS attacks to cause significant damage. Additionally, there have been an increasing number of cases where end customers have approached their providers because they are confronted with blackmail attempts with the threat of a DDoS attack. This was also the case with htp customers. A combination of these trends places higher demands on ISP's for protection against DDoS attacks, but also open up new revenue opportunities as well.

THE CHALLENGE:

While DDoS protection technologies have developed in leaps and bounds over the years, most solutions are only reactive to the threat, and valuable time is lost as a result. Legacy solutions are particularly expensive and most of the time are not able to keep pace with modern DDoS attacks. Traditional scrubbing centers, for example, have an Achilles heel: they rely on a relatively rough sample pattern to analyze the data flow. They "decide" whether or not a DDoS attack is occurring based on this pattern, which can lead to fatal misjudgments. More often than not, it is a successful attack that leads to a more intensive debate on the topic.

Robert Remenyi, responsible for planning the Internet backbone at htp GmbH adds: "About two years ago, we started to examine the peaks of bandwidth measurements. FlowAccounting gives us the opportunity to analyze unusual peaks, and with this process, our investigation confirmed our suspicions. Some DDoS attacks had actually taken place without being detected. These attacks were generally UDP (User Datagram Protocol) amplification attacks, typically using one of the DDoS attack vectors that exploits publicly accessible systems such as poorly configured DNS servers or routers and other vulnerable points."

EVALUATION

Following the activation of general FlowAccounting, it was apparent that there had already been some DDoS attacks, the majority of which were UDP amplification attacks that posed an immediate danger to the htp infrastructure. Not only were parts of central systems in danger, there was also the threat of bottlenecks. "We had to act quickly because we were seeing DDoS attacks occur on a daily basis. As an initial measure, we used comparatively simple static filters on existing routers. These filters are designed to repel or stop attacks that are already known and clearly identified as such. The nature of the data flow suggests that it cannot be legitimate traffic. This measure was extremely effective from the word go. However, solutions of this kind are not capable of defeating new types of intelligent attack. At the same time, we started to look around for solutions that met this attack profile and would be able to satisfy our professional demands", Robert Remenyi explains.

A successful attack that succeeded in making the central system of the carrier temporarily unavailable was the final straw.

THE SOLUTION

Attackers are well aware of the weak points of traditional scrubbing centers and other methods, and have modified their techniques accordingly. If the size of the attack is low, they fly under the radar and prevent the relevant traffic from being redirected. Sample patterns in scrubbing centers are not really suited to identifying the vast majority of modern DDoS attacks, let alone defeating them appropriately.

These days, DDoS attacks can do so much more than "just" interrupt services or prevent access to websites. For more than a year, Corero Network Security has seen a steady increase in the number of short duration, sub-saturating DDoS attacks, which require very little bandwidth.

Consequently, there is a need both to immediately assess whether a security incident is actually occurring and analyze trends in the long term in order to respond quickly to future developments. At htp, the aim was to consistently maintain normal operation using new technology. The system had to have as little influence on the processes at htp as possible, as htp didn't want to have to make constant changes to the technology. All transit connections and the entire underlying infrastructure are now conveniently protected by a single solution.

About a year has passed from the time htp initially contacted various manufacturers to final activation of the production system at the start of August 2016. In order to ensure that the plan could be implemented in the desired way, a proof of concept process was put into place.

The selected solutions for the POC varied from a technical viewpoint. Provider 1 uses a Netflow/Syslog and BGP (Border Gateway Protocol) analysis. Mitigation to filter the attacked IP was achieved using Remotely Triggered Black Hole filtering (RTBH) via an appliance. Here, the routing tables are configured in such a way that any network traffic based on the destination IP address or origin IP address (Source-Based Remotely Triggered Black Holing - SRTBH) is not redirected into the network, but "into thin air". If the destination IP address is used as a filter, the entire flow of data directed towards the target system is discarded. The method is comparatively easy to implement and relatively simple to configure. However, this can also be a disadvantage because by filtering the attacked IP using RTBH, the provider actually helps the attack succeed because the desired data flow will no longer arrive at the server if all data traffic is filtered. The server is therefore

no more accessible than if it were still under attack. In this case, htp regards the second step of diverting the suspect network traffic via a scrubbing center as too complex. In contrast, Corero Network Security and another rival DDoS mitigation provider use the “in-line” method. However, the settings of the third provider also showed signs of weakness, which immediately resulted in false positives. Another shortcoming was that it was not possible to change to monitor mode with this particular solution.

Robert Remenyi added: “Costs actually represented a great consideration in the decision making process. In spite of this, there is no other alternative solution available other than the Corero SmartWall Threat Defense System, that can provide such effective protection against DDoS attacks. The solution is extremely easy to use during operation, partly due to the intuitive user interface. If situations become more complicated, experience shows that we can place our trust in a very reliable and competent support team provided by Corero.

“In the meantime, implementation is now almost complete and we are certain that we will be able to focus much more clearly on our core business in the future instead of being side-tracked by DDoS defense”, said Remenyi. “Our most important objectives were to reduce our daily workload for DDoS defense and automate our defense systems. Here, we are able to benefit from the experience of Corero and their SoC. We were already familiar with the Splunk monitoring feature included in the Corero system and are very pleased with the overall solution”, Remnyi added.

OPPORTUNITIES AND RISKS FOR PROVIDERS

Thanks to modern hardware and software, it is now possible to detect and mitigate modern DDoS attacks in real time.

ISPs are becoming more and more aware of DDoS attacks. At the same time, the pressure is rising. You can easily imagine what would happen to the reputation of a service provider if a customer loses data or a website is no longer accessible as a result of a DDoS attack. Apart from the risk, it gives providers a great opportunity to raise their profile among their customers and set themselves apart from the competition. ISPs should offer their customers a dynamic solution for protecting against DDoS attacks, whereby they only pay for the bandwidth actually used when an attack occurs. htp is already considering offering a service of this kind because they are attractive for end customers.

CONCLUSION

Robert Remenyi draws a preliminary conclusion: “We think that there is actually no alternative to the Corero solution. We are benefiting from the advantages of an automated, distributed approach to DDoS defense. Classic methods and free resources will only get you so far because there is still a dangerous residual risk that DDoS attacks cannot be stopped, in particular new types of attacks. Out of the three options mentioned, we chose the solution that was most suitable for us. The further expansion of Internet uplinks requires us to direct them via anti-DDoS appliances. We are also planning to offer the service to our customers in the future because customers are taking providers up on their promise of providing protection against DDoS attacks to an increasing extent.”

ABOUT CORERO NETWORK SECURITY

Corero Network Security is the leader in real-time, high-performance DDoS defense solutions. Service providers, hosting providers and online enterprises rely on Corero’s award winning technology to eliminate the DDoS threat to their environment through automatic attack detection and mitigation, coupled with complete network visibility, analytics and reporting. This next-generation technology provides a First Line of Defense® against DDoS attacks in the most complex environments while enabling a more cost effective economic model than previously available. For more information, visit www.corero.com

Corporate Headquarters
225 Cedar Hill St.
Suite 337
Marlborough, MA 01752 USA
Phone: +1.978.212.1500
Web: www.corero.com

Germany
Pappelallee 78-79
10437 Berlin Germany
Tel. +49 30 609849 0514