



CASE STUDY

Successfully Defeating Ransom DDoS Attacks





Heinlein Hosting and mailbox.org: Security, Availability, and Data Protection at the Highest Level

As the operator of mailbox.org, Heinlein Hosting GmbH is one of the leading providers of paid email services in Germany. The Berlin-based company also maintains several data centers in Germany and offers its own video conferencing solution called OpenTalk.eu in addition to individual business hosting. Security, availability, and data protection are at the heart of all these services. Email services in particular must be reliable, as electronic communication is extremely time and business-critical these days. Trust plays a decisive role in customer relations here. Every minute of downtime means a drop in sales and leads to a lasting loss of trust and image.

Heinlein therefore decided to protect its email service mailbox.org from DDoS attacks with Myra Security's solutions in addition to internal measures. Due to the successful collaboration, the partners expanded their cooperation to other networks and services in November 2021. Since then, Heinlein Hosting has benefited from overall protection of the underlying infrastructure for all its services thanks to Myra's highly certified, scalable Security-as-a-Service platform. The GDPR-compliant solution from the Munich-based specialist provider meets all the security, performance, and data protection requirements of Heinlein Hosting and its customers.

Starting Point and Goals

The number and complexity of cyberattacks is continuously increasing. According to the German Federal Office for Information Security (BSI), digital blackmail using DDoS and ransomware in particular is booming. Considering the intensified threat situation and known DDoS attacks on other email providers, Heinlein Hosting expanded its preventive infrastructure protection systems at an early stage. To protect its data centers and its email service mailbox.org from attack-related outages, the company decided to implement dedicated DDoS protection for the network and transport layers (layers 3 and 4) in addition to the internal defensive measures already in place.

As Heinlein Hosting hosts all of its services in Germany itself and avoids any collaboration with third-party service providers from non-EU countries for data protection reasons, those responsible were looking for a German DDoS protection provider. In addition to the necessary technical expertise and experience, the requirements profile also included GDPR compliance and local support.

Following independent research and a cooperative exchange of experiences with other email providers, Heinlein Hosting finally contacted Myra Security. "Myra quickly won us over with its technical expertise and very thorough technical discussions at eye level. We immediately had a good feeling," recalls Managing Director Peer Heinlein. Just a few weeks later, the companies signed a multi-year contract for the use of Myra Cloud Scrubbing. The solution protects IT infrastructure and IP subnets against large-volume attacks on layers 3 and 4.

Implementation

Myra DDoS protection for infrastructures and data centers is independent of the existing infrastructure and can be implemented quickly because it requires no additional hardware or software. Myra takes care of almost the entire setup and configuration of the protection solution. The effort on the customer side is minimal.

The customer creates the RIPE route objects for their networks in accordance with Myra's specifications. The Myra Network Operations Center (NOC) team of experts takes care of the


configuration for the networks. In the event of an attack, Myra uses "More Specific" advertisements to pull all incoming traffic to its own scrubbing centers. There, the attack traffic is discarded and the remaining clean traffic is forwarded back to the customer via a previously agreed connection. To automate this switchover, Myra can evaluate the customer's flow data. The customer provides a virtual machine for this purpose, the Myra experts define the threshold values and regularly adjust them with the customer.

For traffic forwarding, direct connections, virtual LAN connections, GRE tunnels and IPSec are available. In the case of Heinlein Hosting, the transfer of clean traffic takes place with multiple redundancy via a direct LAN connection between Myra and the customer infrastructure at the Berlin exchange node BCIX as well as via various virtualized LAN connections.

Summary: Dedicated DDoS Protection Pays off

With the help of the implemented Security-as-a-Service solution from Myra, Heinlein Hosting has successfully fought off several DDoS attacks since the start of the contract. For example, there was a ransom DDoS attack on mailbox.org in mid-October 2021: The SYN flood attack on layer 3/4 lasted several hours and took place in two waves of up to 64 minutes with peak bandwidths of 291 GBit/s and 278 million packets per second, based on a total of almost 150,000 attacking IPs. As the attack bandwidths reached a multiple of the connection bandwidth, the attack would have been impossible to fend off without the support of Myra from Heinlein Hosting.

Thanks to the Myra filter system installed upstream, the attack was successfully mitigated. The services remained "up & running" for the long duration of the attack and were largely uninterrupted from a user perspective. At the end of the day, mailbox.org was able to announce via Twitter (X):

 mailbox_org @mailbox_org · 21. Okt.
DDoS attack ended some time ago. We did not allow ourselves to be blackmailed and did not pay. And we never will.

Typical for ransom DDoS: At the same time as the attack, mailbox.org received a blackmail email. In it, the criminals demanded protection money in Bitcoin and threatened further attacks if payment was not made. One such attack followed the very next day, but was also successfully defended against and had no effect on the operation of mailbox.org. The dedicated DDoS protection thus prevented both serious disruptions and performance losses on the customer side as well as any consequential damage on the provider side, such as loss of image and trust as well as loss of revenue. As a result, the investment in Myra technology paid for itself within a short period of time.

"Communication must function and be available for our customers. That's why DDoS protection measures are not a question of financial considerations, but a necessary basic safeguard either way. Myra delivers top quality made in Germany here," concludes Heinlein Hosting Managing Director Peer Heinlein. "We are very grateful for the first-class human and professional service." Thanks to Myra's scalable anti-DDoS technology, Heinlein Hosting can offer its customers future-proof, compliance-compliant solutions with maximum security, availability and data protection.

By Working with Myra, Heinlein Hosting Benefits from the Following Advantages:

- High availability thanks to Myra's multi-redundant infrastructure
- Low implementation and maintenance costs, as no additional hardware or software is required
- Local 24/7 support from Germany via the Myra-NOC (Network Operations Center) at the headquarters in Munich
- Access to the expertise and industry experience of a highly certified specialist provider
- Certified security in accordance with BSI ISO 27001 based on IT-Grundschutz
- Reliable GDPR compliance

ISO 27001 BSI zertifiziert
auf der Basis von IT-Grundschutz
Zertifikat Nr.: BSI-IGZ-0667-2024



KRITIS
Nachweis gemäß
§ 8a, Abs. 3 BSIG

Certified by the Federal Office for Information Security (BSI) in accordance with ISO 27001 on the basis of IT-Grundschutz | Certified in accordance with Payment Card Industry Data Security Standard (PCI DSS) | Qualified for critical infrastructure in accordance with §3 BSI Act | BSI C5 Type 2 | Certified Trusted Cloud Service | KRITIS operator in accordance with Section 8a (3) BSI Act