MYRA

CASE STUDY

Erpresserische DDoS-Attacken erfolgreich abwehren

Case Study
Heinlein Hosting
(mailbox.org)

Lösungen
DDoS Protection

Heinlein Hosting und mailbox.org: Sicherheit, Verfügbarkeit und Datenschutz auf höchstem Niveau

Die Heinlein Hosting GmbH gehört als Bertreiber von mailbox.org zu den führenden Providern kostenpflichtiger E-Mail-Services in Deutschland. Zudem unterhält das Berliner Unternehmen hierzulande mehrere Rechenzentren und bietet neben individuellem Business Hosting auch eine eigene Videokonferenzlösung namens OpenTalk.eu an. Sicherheit, Verfügbarkeit und Datenschutz stehen bei allen diesen Services im Mittelpunkt. Gerade E-Mail-Dienste müssen zuverlässig arbeiten, da die elektronische Kommunikation heutzutage extrem zeit- und geschäftskritisch ist. Vertrauen spielt hier eine entscheidende Rolle für die Kundenbeziehung. Jede Minute Downtime bedeutet Umsatzrückgänge und führt zu nachhaltigem Vertrauens- und Imageverlust.

Deshalb entschied sich Heinlein, seinen E-Mail-Dienst mailbox.org zusätzlich zu internen Maßnahmen mit den Sicherheitslösungen von Myra Security präventiv vor DDoS-Angriffen zu schützen. Aufgrund der erfolgreichen Zusammenarbeit weiteten die Partner ihre Kooperation im November 2021 auf weitere Netze und Services aus. Seitdem profitiert Heinlein Hosting von einem Gesamtschutz der zugrundeliegenden Infrastruktur für alle seine Dienste durch die hochzertifizierte, skalierbare Security-as-a-Service-Plattform von Myra. Die zu 100 Prozent DSGVO-konforme Lösung des Münchner Spezialanbieters erfüllt alle Ansprüche von Heinlein Hosting sowie seiner Kundschaft an Sicherheit, Performance und Datenschutz.

Ausgangssituation und Zielsetzung

Die Anzahl und Komplexität von Cyberangriffen nimmt kontinuierlich zu. Insbesondere digitale Erpressung mittels DDoS und Ransomware hat laut Bundesamt für Sicherheit in der Informationstechnik (BSI) Hochkonjunktur. Angesichts der verschärften Bedrohungslage sowie bekannt gewordener DDoS-Angriffe auf andere E-Mail-Provider baute Heinlein Hosting seine präventiven Infrastruktur-Schutzsysteme schon frühzeitig aus. Um seine Rechenzentren und seinen E-Mail-Dienst mailbox.org vor angriffsbedingten Ausfällen zu schützen, entschied sich das Unternehmen, zusätzlich zu bereits getroffenen internen Abwehrmaßnahmen einen dedizierten DDoS-Schutz für die Vermittlungs- und Transportschicht (Layer 3 und 4) zu implementieren.

Da Heinlein Hosting seine gesamten Services in Deutschland selbst hostet und aus Datenschutzgründen jede Zusammenarbeit mit Drittdienstleistern aus Nicht-EU-Ländern vermeidet, waren die Verantwortlichen auf der Suche nach einem deutschen DDoS-Schutzanbieter. Zum Anforderungsprofil gehörten neben der notwendigen technischen Expertise und Erfahrung auch 100%ige DSGVO-Konformität sowie lokaler Support.

Nach eigenständiger Recherche und kooperativem Erfahrungsaustausch mit anderen E-Mail-Providern nahm Heinlein Hosting schließlich Kontakt zu Myra Security auf. „Mit seiner technischen Expertise und sehr gründlichen Fachgesprächen auf Augenhöhe hat uns Myra schnell überzeugt. Wir hatten gleich ein gutes Gefühl“, erinnert sich Geschäftsführer Peer Heinlein. Nur wenige Wochen später unterzeichneten die Firmen einen mehrjährigen Laufzeitvertrag über den Einsatz der Myra DDoS BGP Protection. Die Lösung schützt IT-Infrastruktur und IP-Subnetze vor großvolumigen Angriffen auf Layer 3 und 4.

Umsetzung

Der Myra DDoS-Schutz für Infrastrukturen und Rechenzentren ist unabhängig von der bestehenden Infrastruktur und kurzfristig implementierbar, weil er keine zusätzliche Hard- oder Software erfordert. Myra übernimmt nahezu die komplette Einrichtung und Konfiguration der Schutzlösung. Der Aufwand auf Kundenseite ist minimal.

Der Kunde erstellt die RIPE-Route-Objekte für seine Netze gemäß der Vorgaben durch Myra. Um die Konfiguration für die Netze

kümmert sich das Expertenteam des Myra Network Operations Center (NOC). Mittels „More Specific" Annoncierungen zieht Myra im Angriffsfall den kompletten eingehenden Traffic auf die eigenen Scrubbing Center. Dort wird der Angriffstraffic verworfen und der verbleibende saubere Traffic über eine vorher vereinbarte Verbindung dem Kunden wieder zugeleitet. Um diese Umschaltung zu automatisieren, kann Myra die Flow-Daten des Kunden auswerten. Dafür stellt der Kunde eine virtuelle Maschine zur Verfügung, die Myra-Fachleute übernehmen die Definition der Schwellenwerte und gleichen diese regelmäßig mit dem Kunden ab.

Für die Traffic-Weiterleitung stehen direkte Verbindungen, virtuelle LAN-Verbindungen sowie GRE-Tunnel und IPSec zur Verfügung. Im Fall von Heinlein Hosting erfolgt die Übergabe des Clean-Traffics mehrfach redundant sowohl über eine direkte LAN-Verbindung zwischen Myra und der Kundeninfrastruktur am Berliner Austauschknoten BCIX als auch über verschiedene virtualisierte LAN-Verbindungen.

Resümee: Dedizierter DDoS-Schutz zahlt sich aus

Mithilfe der implementierten Security-as-a-Service-Lösung von Myra hat Heinlein Hosting seit Vertragsbeginn mehrere DDoS-Attacken erfolgreich abgewehrt. Beispielsweise kam es Mitte Oktober 2021 zu einem erpresserischen DDoS-Angriff auf mailbox.org: Die mehrstündige SYN-Flood-Attacke auf Layer 3/4 erfolgte in zwei Wellen von bis zu 64 Minuten mit Spitzenbandbreiten von 291 GBit/s und 278 Millionen Paketen pro Sekunde, ausgehend von insgesamt knapp 150.000 attackierenden IPs. Da die Angriffsbandbreiten ein Vielfaches der Anbindungsbandbreite erreichten, wäre die Attacke ohne Unterstützung durch Myra von Heinlein Hosting allein nicht abzuwehren gewesen.

Dank des vorgeschalteten Myra-Filtersystems wurde der Angriff aber erfolgreich mitigiert. Die Services blieben auch über die lange Zeit des Angriffs „up & running" und aus Anwendersicht weitgehend störungsfrei. So konnte mailbox.org am Ende des Tages via Twitter verkünden:

Für DDoS-Erpressung typisch: Zeitgleich mit dem Angriff erhielt mailbox.org eine Erpresser-Mail. Darin forderten die Kriminellen ein Schutzgeld in Bitcoin und drohten bei Nichtzahlung mit weiteren Angriffen. Ein solcher folgte gleich am nächsten Tag, konnte aber ebenfalls abgewehrt werden und blieb wirkungslos auf den Betrieb von mailbox.org. Der dedizierte DDoS-Schutz verhinderte somit sowohl schwere Störungen und Performance-Einbrüche auf Kundenseite als auch etwaige Folgeschäden auf Anbieterseite wie Image- und Vertrauensverlust sowie Umsatzeinbußen. Dadurch hat sich die Investition in die Myra-Technologie schon nach kurzer Zeit amortisiert.

„Kommunikation muss für unsere Kundinnen und Kunden funktionieren und verfügbar sein. Daher sind DDoS-Schutzmaßnahmen keine Frage einer finanziellen Abwägung, sondern eine so oder so notwendige Grundabsicherung. Myra liefert hier Spitzenqualität made in Germany", so das Fazit von Heinlein-Hosting-Geschäftsführer Peer Heinlein. „Wir bedanken uns sehr für den menschlich wie fachlich erstklassigen Service." Dank der jederzeit skalierbaren Anti-DDoS-Technologie von Myra kann Heinlein Hosting seinem Kundenkreis zukunftssichere, Compliance-konforme Lösungen mit einem Höchstmaß an Sicherheit, Verfügbarkeit und Datenschutz anbieten.

Durch die Zusammenarbeit mit Myra profitiert Heinlein Hosting von folgenden Vorteilen:

- höchste Verfügbarkeit durch mehrfach redundante Infrastruktur von Myra
- geringer Implementierungs- und Wartungsaufwand, da keine zusätzliche Hard- und Software erforderlich ist
- lokaler 24/7-Support aus Deutschland über das Myra-NOC (Network Operations Center) am Hauptsitz in München
- Zugang zu Expertise und Branchenerfahrung eines hochzertifizierten Spezialanbieters
- zertifizierte Sicherheit nach ISO 27001 auf Basis von IT-Grundschutz des BSI
- Rechtssichere DSGVO-Konformität

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | BSI C5 TESTAT TYP 2 | Trusted Cloud SERVICE | CERTIFIED IDW PS 951 ISAE 3402 | DIN EN 50600 zertifiziert BETRIEBSSICHERES RECHENZENTRUM

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard (PCI DSS) | KRITIS-qualifiziert nach §3 BSI-Gesetz | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600