Picture Credits: newsroom.hermesworld.com

CASE STUDY: HERMES GERMANY GMBH

DDOS-ATTACKEN LASSEN HERMES KÜNFTIG KALT

VON HARRY WEILAND

DDoS-Abwehr aus der Cloud: Die Hermes Germany GmbH schützt ihre gesamte IT-Infrastruktur und alle relevanten Webanwendungen rund um die Uhr mit Link11. Als europaweit agierender Logistikdienstleister mit vielen Kunden und Partnern will es sich das 12.000 Mitarbeiter große Unternehmen nicht leisten, seine IT vor DDoS-Gefahren ungeschützt zu lassen. Konkrete Ereignisse setzten das Thema Cyberkriminalität bei Hermes auf die Tagesordnung.

Kaum eine Branche ist so hochgradig vernetzt wie die Logistik, besonders – wie Hermes Germany – im B2C-Bereich. Mehrere hundert Großkunden, Millionen Privatkunden und 15.000 Paketshops allein in Deutschland bilden bei Hermes ein großes Netz, in dem sekündlich Millionen Daten in alle Richtungen versendet werden. Elektronische Schnittstellen zu Lieferanten, Kunden und Zustellern verfeinern das Ganze.

Sicherheit in der IT ist für Hermes Germany kein neues Thema. Gegen klassische Gefahren aus dem Internet ist die Tochtergesellschaft des Otto-Konzerns seit langem gewappnet. 2017 aber kam eine neue Gefahrenquelle hinzu: Cyberkriminalität mit Hilfe von DDoS-Attacken. Hermes hatte bislang keine explizite DDoS-Schutzlösung im Einsatz. „Es gab Ereignisse, die uns gezeigt haben, dass DDoS-Attacken ein reales Risiko sind“, berichtet Alexander Sölter, IT-Service-Manager bei Hermes Germany. Das Bewusstsein für das Thema war fortan vorhanden und es gab „auch kein Zurück mehr“, sagt Alexander Sölter. Hermes suchte fortan nach einem Partner, der dem Unternehmen helfen sollte, Distributed-Denial-of-Service-Angriffe (DDoS) auf die Server des Hauses zu verhindern.

Priorität hatte dabei der Schutz der gesamten Netzwerkinfrastruktur des Unternehmens, etwa VPN-Server, Mail-Server und Firewalls. Die Abwehr von DDoS-Attacken auf die vollständige IP-Range des Unternehmens und der Domains mit den dahinterliegenden Webwendungen sollte unmittelbar in einem zweiten Schritt erfolgen.

Hermes sah sich mehrere Anbieter an, entschied sich aber schnell für Link11. Deutscher Datenschutz, die räumliche Nähe zwischen Frankfurt und Hamburg und die gute Erreichbarkeit waren die ersten Pluspunkte, die aus Sicht von Hermes für Link11 sprachen. „Unkompliziert, direkt und schnell“, schildert Alexander Sölter seinen frühen Eindruckvon Link11. Die Vertreter des mehrfach mit Preisen

ausgezeichneten Anbieters aus Frankfurt am Main hätten einen positiven Eindruck hinterlassen, nicht nur in Sachen Produkt und Prozesse, sondern auch was das Verständnis des Themas angeht. Referenzen aus der Logistik waren für Alexander Sölter und seine Kollegen ein weiterer Pluspunkt für Link11. Vor allem aber gefiel den Hamburger Logistikern Link11, weil der „Internet-Türsteher“ sofort helfen konnte. Hermes brauchte eine schnelle Lösung und Link11 konnte in kurzer Zeit die Hermes-Netzwerkinfrastruktur über das Border Gateway Protocol (BGP) so schützen, dass ad hoc Gefahren gebannt waren, berichtet Alexander Sölter. „Das war in dem Moment genau das, was wir gebraucht haben.“

Bei Hermes fand man auch einen Gefallen daran, den Schutz gegen DDoS-Crime in die Hände eines Anbieters zu legen, der sich im Gegensatz zu einem klassischen Internet Service Provider auf das Thema spezialisiert hat. Hermes vertraut darauf, dass Link11 mit seinem eigenen mit künstlicher Intelligenz unterstütztem Schutz-Algorithmus die globale DDoS-Gefahrenlage jederzeit umfassend im Blick hat und dabei einen automatischen und proaktiven Schutz bieten kann. Der Logistiker aus Hamburg will nicht von seinem DDoS-Sicherheitsanbieter zum Handeln aufgefordert werden, sondern er erwartet, dass derlei Angriffe im Vorfeld abgewehrt werden und das Unternehmen gar nichts damit zu tun hat. Sölter: „Es kommt für uns nicht in Frage, erst etwaige Bedrohungen zuzulassen und dann erst zu reagieren.“ Hermes wollte künftig 24/7 Schutz vor DDoS-Attacken haben, ohne sich um das Thema kümmern zu müssen.

Aus diesem Grund hat sich Hermes Germany für den permanenten DDoS-Schutz von Link11 entschieden. Die gesamte Netzwerkinfrastruktur von Hermes ist dauerhaft über redundante Layer-2-Verbindungen an das Link11-Filterzentrum angebunden. Der Internetverkehr der Infrastruktur ist mittels Border Gateway Protocol dauerhaft über Link11 geroutet. Jeglicher Internetverkehr kann somit in Echtzeit von DoS/DDoS Angriffen gesäubert werden, um den legitimen Verkehr dann über die Layer-2-Verbindungen an Hermes zu übergeben. Ein dauerhafter Schutz auf den Ebenen Layer 3 und 4 ist so für den gesamten IP Adress-Bereich gewährleistet.

Um kritische Webanwendungen von Hermes (etwa www.myhermes.de) bis auf Layer 7 vor DDoS-Angriffen zu schützen und selbst verschlüsselten Attacken habhaft zu werden, werden diese Anwendungen zusätzlich noch über spezielle Proxies in der Link11 Security Cloud umgeleitet. "Wir haben nun Technologien zum bestmöglichen Schutz und gleichzeitig keine Latenzverzögerungen", bilanziert Alexander Sölter.

Die Kombination des cloudbasierten 360-Grad-Schutzes von Link11 mit der Hermes-Infrastruktur hatte ihre Herausforderungen, zumal Hermes-Partner weltweit mit unterschiedlichen Schnittstellen an ihren Logistik-Dienstleister angebunden sind. „Diese Themen wurden erfolgreich abgearbeitet“, sagt Alexander Sölter. Die Kommunikation mit dem Security-Dienstleister funktioniere ohnehin gut, die Antwortzeiten per Mail und dankenswerterweise auch per Telefon „erfüllen unsere Erwartungen“.

„Wir befinden uns in regelmäßigem Austausch“, lobt Alexander Sölter, man besucht sich immer wieder und bringt sich gegenseitig auf den aktuellen Stand. Vorteil für Hermes: Man erfährt, was sich außerhalb des eigenen Kosmos tut und auf welche Themen man sich künftig eventuell einzustellen hat. Und der Schutz? Der funktioniert wie versprochen – heißt es bei Hermes. „Wir haben seit der Installation von Link11 als Türsteher keine weiteren Angriffe auf unser Netz mehr gehabt“, sagt der Hermes-Verantwortliche. Bei Link11 würden hingegen durchaus regelmäßig Angriffsversuche auf die IP-Bereiche von Hermes registriert. Link11 mitigiert die Attacken und liefert entsprechende Berichte dem Kunden, so dass dieser immer über die aktuelle Gefahrensituation im Bilde ist.

Wurde Sölter früher telefonisch oder per Mail über derlei Angriffe informiert, ist er heute glücklich, dass es nun eine moderne Lösung für diesen Informationsaustauch gibt. Die neue Link11 WebGUI erlaubt ihm künftig einen eigenen Blick auf abgewehrte DDoS-Angriffe, Server-Verfügbarkeiten und -Antwortzeiten. Sölter: „Die WebGUI ist sehr hilfreich.“

Das Fazit bei den Hamburger Logistikexperten:
Link11 punkte mit Expertise, Flexibilität und Agilität. Der Logistikriese fühlt sich bei den Schutz-Experten gut aufgehoben. Alexander Sölter: „Das Vertrauen war sehr schnell da und es ist bis heute nicht enttäuscht worden.“