LINK11

CASE STUDY

GLS.

www.link11.com

Protecting logistics across Europe: How GLS is protecting its parcel flow from DDoS attacks with Link11

At a time when targeted cyberattacks are posing an increasing threat to the parcel service industry, logistics giant GLS has taken urgent measures to protect its critical infrastructure. Faced with the risk of massive operational disruptions and potential financial damage, GLS, after a systematic evaluation, implemented Link11 to ensure the stability of all business-critical processes.

A European force to reckon with in logistics

General Logistics Systems B.V. (GLS), headquartered in Amsterdam, is one of the leading international logistics service providers. Founded in 1999, GLS has developed into one of the most reliable parcel service networks in Europe and North America. With around 23,000 employees, over 120 central hubs, and more than 1,600 depots, the company serves approximately 240,000 customers. Its annual parcel volume is an impressive 926 million.

Group IT acts as an internal IT service provider, ensuring the smooth operation of the entire infrastructure. Christof Weppler, Senior IT Infrastructure Architect, is responsible for the strategic development of the network infrastructure. For him and the company, the highest possible availability of key services is paramount.

An industry targeted by attackers

When a wave of targeted attacks recently hit the parcel service industry and the threat situation escalated dramatically, it became evident that manually responding to incidents was no longer sufficient.

The mere possibility of a total failure, which would significantly disrupt the flow of parcels and have serious economic consequences, made investing in a professional protection solution unavoidable. It was no longer a question of whether DDoS protection was needed, but how quickly it could be implemented in the best possible way. According to Christof Weppler, the urgency was immediately recognized: “Time has shown that we cannot do without comprehensive protection.”

“Time has shown that we cannot do without comprehensive protection.”

Christof Weppler, Senior IT-Infrastructure Architect

Systematic search for optimal protection

The manual and rather impractical temporary solution used by GLS was unsustainable in the long term. In 2020, this led to the strategic decision to explore the market for permanent, automated protection. From the outset, only an automated, cloud-based solution would be considered. “Attacks are constantly evolving,” explains Christof Weppler. „In the worst case, an on-premises solution may not even be effective or able to withstand the volume of the attack. There was no alternative to choosing a cloud provider.“

Christof Weppler conducted a structured evaluation and compared different providers. Beyond this process, several fundamental characteristics were of crucial importance:

- A partnership-based approach: The GLS team explicitly preferred a flexible provider that would engage as an equal partner in order to avoid rigid processes. Being taken seriously as a customer was crucial.
- Qualified, accessible support: A direct line to competent contact persons, without long waiting times, was a must.
- Performance and data sovereignty: Traffic should remain within Europe, additionally the provider should be GDPR-compliant and have sufficient bandwidth to fully secure the connections.
- Price and reputation: The price-performance ratio also played an important role, as did reputation. The search was on for a well-known provider; Link11‘s awards contributed positively to the evaluation.

Link11 stood out as the strongest overall solution. The company best met GLS‘s key requirements and was awarded the contract after the final evaluation in 2020.

From reactive action to proactive collaboration

Since then, GLS has described its collaboration with Link11 as positive and constructive. Those responsible at GLS particularly appreciate the feeling of being taken seriously as a customer and not being caught up in rigid processes. Feedback from GLS is implemented quickly and confidently within the scope of the given possibilities.

The appreciation is mutual, as Stefan Haupter, Key Account Manager at Link11, confirms: “You can immediately tell that GLS has real experts at work. They know exactly which systems and processes are business-critical and therefore need to be prioritized for protection. Together, we act as the first line of defense to identify and mitigate threats.”

Even after five years of partnership, regular discussions take place between GLS and Link11 to discuss traffic patterns and anomalies – an exchange that GLS considers very valuable. This active collaboration is also reflected in the direct and uncomplicated contact, which, if necessary, extends to the management level of Link11.

Operational security, peace of mind, and full focus on the core business

Since implementing the Link11 DDoS protection solution, GLS feels secure when it comes to its own IT infrastructure. The collaboration is characterized by a continuous optimization process. If necessary, the parameters are adjusted in close cooperation with Link11 support to precisely meet the needs of GLS in order to ensure the best possible protection at all times.

The greatest added value lies in the stability gained: the lines to the data center that are critical for packet flow, VPN, and SD-WAN remain free and protected. This knowledge provides GLS with the necessary peace of mind.

“Now that we know that the products we have are good and that no attacks can get through, we can sleep more soundly.”

Christof Weppler, Senior IT-Infrastructure Architect

DDoS protection is no longer a topic of discussion at GLS, but – just like virus protection – an established standard. The investment in Link11 has proven to be a strategic decision for the resilience of the entire core business.

LINK11

Link11 is a German IT security provider specializing in DDoS protection and cyber resilience. The company operates a high-performance, AI-powered protection system that detects and automatically defends against attacks in real time. Link11 is BSI-certified, ISO 27001-compliant, and offers security solutions “Made in Germany” that are used worldwide.

Link11 GmbH | Lindleystr. 12 | 60314 Frankfurt | info@link11.com | +49 69 26492977