CASE STUDY GENESYS INFORMATICA

"SAVED IN HOURS"

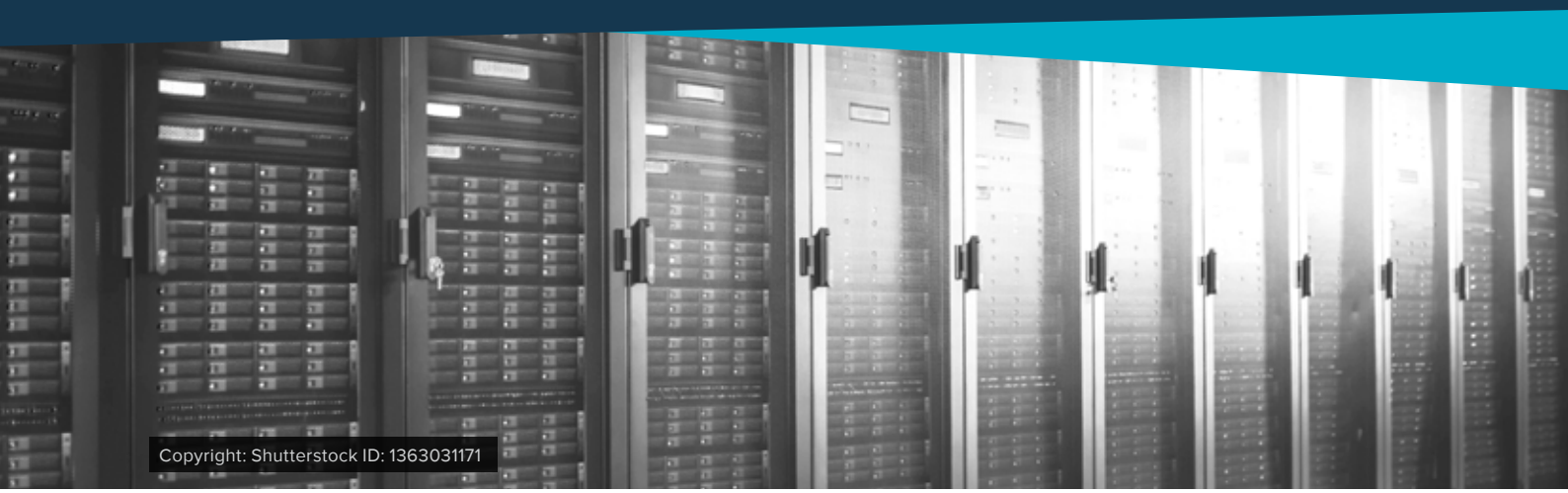
Emergency deployment in Italy: Italian internet service provider Genesys Informatica was helped by Link11 to successfully repel a very large DDoS attack in May 2019. The infrastructure protection provided by Link11 was deployed within just a few hours to the Italian ISP. Genesys Informatica was then able to fend off one of the largest DDoS attacks in Italian history. Stefano Fiaschi, Manager Cloud Computing at Genesys, has this advice to all of his colleagues and peers world-wide: “You have to stay alert at all times to ensure DDoS protection; never rest on your laurels or be complacent about security.”

Genesys, based in Florence, had always anticipated and prepared itself for DDoS attacks but the actual size of the onslaught in 2019 was still a surprise. "It was like an earthquake which shook our infrastructures" reports Stefano Fiaschi. The massive DDoS attacks in May 2019 impacted the company’s nation-wide operations. Until then they relied on their uplink-provider DDoS protection. However, its protective bandwidth was not sufficient on this particular day because of the outstanding entity of the attack. Genesys’ systems were only providing a fraction of their normal performance capacity. If too many attacks hit the uplink-provider simultaneously, this can hit other customers on the same platform or all data traffic is rejected in total by so-called ‘black hole’ routing.

For an ISP like Genesys, this kind of situation is doubly bad because it can affect several thousand customers. And Genesys is not a small player in the Italian market. The ISP, which provides services primarily to SMEs, is one of the top ten hosting providers in Italy. The Tuscany-based company also provides services to many public companies and major players in the property sector.

The attack forced Genesys to act quickly. CEO Luigi Corbacella and his team swiftly contacted providers of DDoS protection systems. It soon reached an understanding with Link11, an internationally active German-based provider. Link11 services include permanent infrastructure protection, the ideal product for Genesys: contractual details were negotiated by the afternoon, while in parallel the entire infrastructure and all traffic managed by Genesys were rapidly placed under the protective shield provided by Link11. After a very busy Friday evening, full DDoS protection had been realised by 1am, early Saturday morning. Genesys' problem was solved, a difficult situation handled. Stefano Fiaschi: "Everyone breathed a sigh of relief."

Genesys was very impressed by the speed at which the problem was resolved. "We had not expected things to happen so fast," admits Stefano Fiaschi. Link11 experts were "efficient and professional", providing support to their



new Italian customer of just a few short hours. Ongoing activities since those dramatic days in May are described by Stefano Fiaschi as being "responsive and cooperative". Issues are quickly handled, with Link11's Frankfurt HQ normally responding no later than the following day.

The Florence-based ISP is happy with its "made in Germany" DDoS protection. Since changing to Link11, no more attacks have got through to Genesys data centres. Every few weeks attacks of several minutes duration are registered, but the attackers quickly realise that they are getting nowhere and back off. Stefano Fiaschi: "The protective shield works."

His company intends to keep upgrading the protection shield capabilities. Stefano Fiaschi: "It is getting easier and cheaper for aggressors to organise massive attacks, we always have to be one step ahead. " Which is why in the future Genesys has contracted Link11 to provide an even bigger guaranteed bandwidth.

The Italian IT experts have learned a lesson from the attacks: while knowing attacks could happen, they had assumed that the protection offered by their connection-provider would be enough. Stefano Fiaschi advises colleagues in other companies not to underestimate the possibility of DDoS attacks. “The enemy is continuously upgrading their efforts, and we must keep apace and stay alert.”

One aspect of collaboration between Genesys and Link11 means that Genesys also benefits from the network expertise of the Frankfurt-based protection specialists. Link11 automatically provides its customers with tips and support to continuously optimise networks and hardware. Genesys is currently establishing a physical link from its own data centres to the Zurich internet exchange point. Since Zurich is also a Link11 filter site, latencies are reduced to a barely discernible minimum. CEO Luigi Corbacella: "The connection to Zurich is one more performance plus for our customers."

Genesys was able to turn a brief crisis in 2019 into a success. It did this by adopting an open and honest communications policy immediately after the incident. Genesys invited its key accounts to an "open day" in Florence. They explained the whole story and introduced their new anti-DDoS partner. This was applauded by customers, reports Luigi Corbacella. "Every customer understood that and said we had done the right thing." With only a few exceptions, most customers remained loyal to their internet service provider. CEO Luigi Corbacella: "We are now stronger than before the crisis, and our new DDoS protection by Link11 helped us."