Fight against cyber attacks enters the next round:

DE-CIX receives patent for new service "Blackholing Advanced"

Frankfurt am Main, **18 April 2021.** DE-CIX, the operator of the world's largest Internet Exchange[1], located in Frankfurt, Germany, has been granted a patent for its new "Blackholing Advanced" service. Blackholing Advanced revolutionizes the defense against DDoS (Distributed Denial-of-Service) attacks directly at Internet Exchanges by using individual filtering mechanisms. This patented mechanism significantly limits malicious traffic at the transport protocol and port level through fine-grained filtering. The patent is valid in Germany, and the application is pending in the USA.

The new service is now available free of charge in a beta version for all DE-CIX customers in Frankfurt, Madrid, and New York. This means that DE-CIX is in direct exchange with its customers in order to bring the product to final market maturity via the beta version. The path from a prototype to a beta version and on to the final product is generally not unusual for technical companies: Google's Gmail, for example, was in active beta for three years.

"We have always developed new services in dialog with our customers, and we also jointly developed the product requirements for Blackholing Advanced in a community workshop. Now, for the first time, we have the opportunity to fully test a beta version, and through this process we hope to receive valuable direct feedback. The patent granted for the innovative filter mechanisms is reward for our years of research, as well as continuous market observation and needs analyses. In times of increasing DDoS attacks, security is an ongoing focus for us and our customers," said Dr. Thomas King, Chief Technology Officer at DE-CIX.

---

[1] Measurement based on the total amount of data throughput in 2020: 25 Exabytes (EB)

Blackholing Advanced: technical background

The patented mechanism gives customers the ability to filter unwanted DDoS traffic at the transport protocol and port level with fine granularity, and in so doing significantly limit harmful data throughput. Based on this filtering, traffic on the award-winning DE-CIX Apollon platform is either discarded or appropriately limited to protect critical infrastructures on the Internet from DDoS attacks. The fact that DDoS data traffic can not only be blocked but also limited in terms of data throughput means that it is possible to investigate the DDoS attack further in order to initiate appropriate countermeasures. Together with the new DE-CIX blackholing dashboard, this enables precise and informed mitigation of DDoS attacks to completely eliminate the unwanted traffic only.

The new service will also be offered as a premium variant in the future. Standard Blackholing Advanced is free of charge for DE-CIX customers and includes numerous preset filters. The high-end Freemium version, which is subject to a charge, also offers flexibly customizable filters that can be activated directly by the customer.

# # #