bugshell – Real cyberattack prevention

IT-security alert - the German economy loses 223 billion euros as a result of hacker attacks.[1] While three quarters of all companies were affected in 2018 to 2019, 90 percent of all German companies fell victim to data theft and damage to IT infrastructure in 2021.[2] Extortion incidents, data corruption, failing production systems, and disruption of operating processes - they are all the direct result of ransomware attacks, which ensure that sensitive files and information are encrypted and rendered unusable. In addition, there are DDoS attacks, where the attackers overload the company's own servers with mass requests in order to shut down the system. German SMEs are aware of these challenges, but hardly know how to defend themselves; after all, one in ten companies have already experienced existential distress according to the Bitkom survey. This is where the Berlin-based cyber security start-up bugshell comes in to protect the German Mittelstand from data leaks and production downtimes with a community of some of Europe's most accomplished cyber security experts and penetration testers.

Penetration testing medium-sized businesses

The German Mittelstand have long been pushing ahead with digitization efforts, but malicious attacks on old and new IT infrastructures are on the rise. Companies are striving for sustainable growth and see the security of their own information systems as the key to a successful
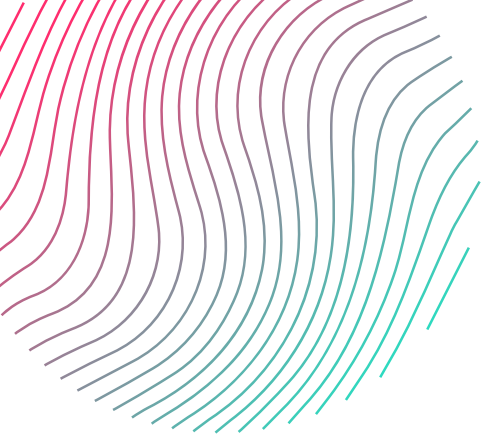
future. For this reason, bugshell offers its customers the execution of so-called penetration tests. Using this method, individual computers, software, web applications, or IT infrastructures such as networks can be specifically checked for potential vulnerabilities. Customers of bugshell hire their IT-security experts to check and identify vulnerabilities using three approaches: Full knowledge of the IT infrastructure (white box), restricted knowledge (grey box) or without any knowledge (black box). Bugshell enables clients, such as companies, CTOs or other technical directors, with suitable cybersecurity experts via a matching process. An additional project management team ensures the execution of the "pentest" and thus provides a high-quality service.

The project progress can be monitored in real time via the platform. This allows clients and experts to communicate on each vulnerability that has been identified so that it can be closed quickly. At the end of a project clients receive a report that mentions, analyzes, and provides a solution for every vulnerability that has been identified throughout the project. All data is stored on European servers under the highest data protection and security standards.

In addition, bugshell supports companies with phishing simulations, consulting, and workshops. For companies, bugshell thus offers an efficient alternative to non-transparent IT security services and provides an independent security pledge through external IT experts.

„Security by Community" – IT security made in Europe

The company taps into its own European community of best-in-class experts in the field of IT security. The individual testers have many years of experience within large companies and are extensively trained with regard to hacking attacks. An in-depth verification process examines the professionalism, experience, and know-how of the experts before assigning them to their respective projects and clients. The platform enables IT professionals to organize their assignments, acquire clients, schedule penetration tests, and ease the process of writing reports.

Bugshell: One vision, two companies, three founders

Bugshell was launched in August 2021 by the initial founding team Jakob Semmler and Volker Haupt. Looking for additional expertise to build the platform, they approached Inko Lorch, who happened to already work on a similar vision with PentServ. Convinced by the idea behind bugshell, he also joined the management team and is now responsible for the technical development of the platform as Chief Technology Officer. Together, they are committed to enabling companies to move towards a safer digital world and to providing cybersecurity professionals a stable source of income, a community to exchange knowledge, and quality of enhancements.

Sources: 1.) Bitkom2022, 2) Tagesschau2021