



Customer use case

What's visible can be attacked. Carletto checks its digital exposure

At a glance

Challenges

- SME with limited internal IT resources
- Distributed infrastructure with webshops, interfaces and VPNs
- Dependent on IT partner for insights into the security posture

Benefits

- Clear visibility into company's digital attack surface
- Identification of forgotten or outdated systems
- Useful documentation for both internal and external stakeholders



«You get a solid picture of the attack surface in no time – without a big project. For us, it was the right move.»

Karin Glaus
CIO

About Carletto

Carletto is an owner-managed B2B distributor of toys based in Brunnen and with an office in Nuremberg. For over 35 years, the company has supplied the retail sector across the DACH region with beloved brands like Steiff, Sigikid, HABA, Pokémon and their own Game Factory label. With some 13,000 articles and a broad e-commerce presence, IT security is an important part of their operations.

Challenge

Carletto operates two webshops and relies on a long-standing IT partner for infrastructure and security. In the face of ever-increasing cyber risks, Carletto wanted to know: What systems were actually visible from the outside? Were there outdated systems, misconfigured domains or forgotten test environments that might be exposed online and present a cyber risk? To gain clarity, Carletto chose GObugfree's Attack Surface Analysis (ASA).

Benefits

External reality check

The ASA revealed which systems were publicly accessible – including a legacy FTP server and a misconfigured DNS entry, both of which were resolved immediately. The assessment also included checks for known CVEs and verified whether available patches had been consistently implemented.

Transparency – internally and externally

The report served as a neutral assessment of the company's security posture – a helpful basis for conversations with the IT provider and documentation for cyber insurance purposes.

Efficient and practical

For a medium-sized company without a dedicated security team, the ASA offered a lightweight, resource-friendly way to assess risk – no major project setup required.