



### Customer use case

## Was digital sichtbar ist, kann angreifbar sein. Carletto prüft ihre Angriffsfläche

### Kurz & bündig

#### Herausforderungen

- KMU mit begrenzten IT-Ressourcen
- Verteilte Infrastruktur mit Webshops, Schnittstellen, VPNs
- Abhängig auf Aussagen des IT-Partners zur Sicherheitslage

#### Nutzen

- Klare Sicht auf die digitale Angriffsfläche
- Aufdeckung vergessener oder veralteter Systeme
- Nachweis für IT-Partner und Cyber-Versicherung



**«Man bekommt in kurzer Zeit ein fundiertes Bild der Angriffsfläche – ganz ohne Grossprojekt. Für uns war das der richtige Schritt.»**

**Karin Glaus**  
CIO

### Über Carletto

Carletto ist ein inhabergeführter B2B-Distributor für Spielwaren in der DACH-Region mit Sitz in Brunnen und einer Niederlassung in Nürnberg. Seit über 35 Jahren beliefert das Unternehmen den Detailhandel mit Marken wie Steiff, Sigikid, HABA, Pokémon und der Eigenmarke Game Factory. Mit rund 13'000 Artikeln und einer breiten E-Commerce-Präsenz ist IT-Sicherheit ein wichtiger Bestandteil der Unternehmensstrategie.

### Herausforderung

Carletto betreibt zwei Webshops und setzt auf einen IT-Partner für Infrastruktur und Sicherheit. Angesichts der zunehmenden Cyberrisiken wollte Carletto wissen: Was ist eigentlich von aussen sichtbar? Gibt es alte Systeme, falsch konfigurierte Domains oder vergessene Testumgebungen, die über das Internet erreichbar sind, und so als potenzielle Angriffsfläche dienen könnten? Um Klarheit zu gewinnen, entschied sich Carletto für eine Attack Surface Analyse (ASA) mit GObugfree.

### Nutzen

#### Realitätscheck von aussen

Die ASA zeigte, welche Systeme öffentlich sichtbar waren – darunter ein veralteter FTP-Server und ein fehlerhafter DNS-Eintrag. Beides wurde umgehend behoben. Die Analyse umfasste zudem Prüfungen auf bekannte CVEs und überprüfte, ob verfügbare Sicherheitsupdates konsequent implementiert wurden

#### Transparenz schaffen – intern und extern

Der Report diente als neutrale Einschätzung der Sicherheitslage – eine wertvolle Grundlage für den Austausch mit dem IT-Partner und als Nachweis für aktives Risikomanagement gegenüber der Cyber-Versicherung.

#### Pragmatisch und effizient

Für ein mittelgrosses Unternehmen ohne eigene Security-Abteilung war die ASA ein ressourcenschonender Einstieg in externe Sicherheitsprüfungen – ohne aufwändiges Projekt.