bugcrowd

CASE STUDY

MANAGED BUG BOUNTY

Bug Bounty integrations reduce vulnerabilities for TX Group

Industry

Media

Challenge

TX Group manages over 500 developers in 50+ locations and is constantly launching new digital products and services. Media organizations are the subject of intense cyber threats, and audits are of limited value.

Solution

Managed Bug Bounty

Outcomes

- Discovery/resolution of up to 20 times more vulnerabilities than discovered by traditional audit processes
- Increased cost/benefit over time as assets have become more secure

About TX Group

Headquartered in Zurich, TX Group AG (formerly Tamedia AG) is the largest private media group in Switzerland. It publishes a portfolio of daily and weekly newspapers, magazines and digital platforms which, collectively, reach over 80 percent of the Swiss population every day. One of its titles alone — *20 Minuten*, a free newspaper available at every Swiss train station and every stop, as well as via a digital portal — reaches 60% of the population every week.

Background Information

The integrity of an independent media company is one its most valuable assets, and an asset to be protected at all costs.

Day-to-day, integrity manifests as objectivity, accuracy and fearlessness: from editorial principles to individual reports.

But such attributes often result in media companies shining a light on issues and places that others — often the subject or their supporters — would prefer to remain hidden. They are, therefore, frequently the target of cyber attacks, with attackers aiming to disrupt reporting, or even to blackmail the publisher via ransomware.

TX Group's approach to security

Given their 'prime target' status, media companies must be extra-vigilant in order to protect themselves. And this is a considerable challenge for TX Group which, among its 3,700 staff and across all its individual companies, employs 500 developers at 50 locations worldwide.

Organization
TX Group's approach to security is headed by Olivier Martinet, Group CISO. He took over from Andreas Schneider who initiated the Bug Bounty program initiative with Bugcrowd. Olivier is supported by **"security champions"**, consisting mainly of Security Officers or DevOps Engineers. Olivier acts as a sponsor, transferring to each business unit his knowledge of establishing security environments and pushing for bug bounty programs. As a result, the bug bounty programs are driven by the individual teams' business units, and centrally coordinated by Olivier.

Culture
While decision-makers in the DACH region are usually very conservative and averse to discussing IT security, TX Group has fostered a culture of talking openly about it.

For example, in November 2020 the company was subjected to DDoS attacks every day, every night. Rather than hide it, TX Group talked publicly about it. The result was that other media companies confirmed that they had been attacked as well, and information was exchanged about how to cope and ramp-up DDoS protection.

TX Group's open-minded approach is behind its adoption of bug bounty programs as a strategy for improving security. The company runs two Public Bug Bounty programs and is one of the few companies in Switzerland doing this.

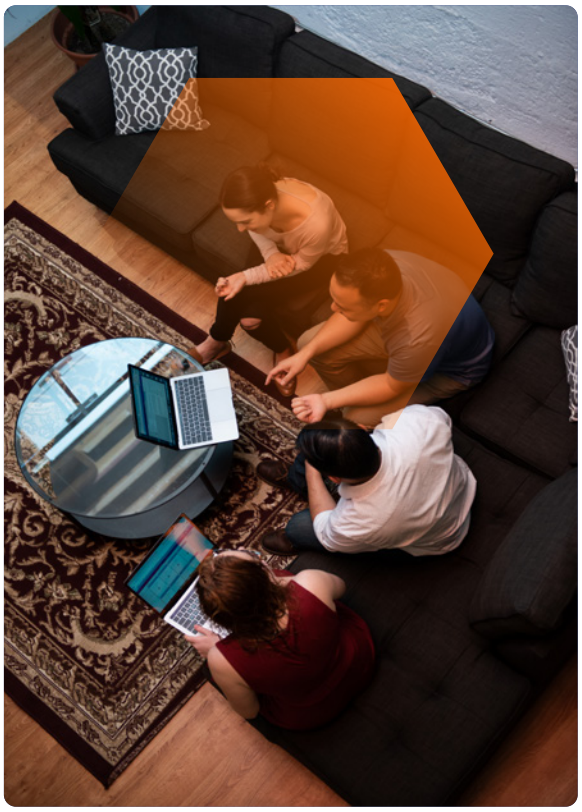
Security challenges leading to a bug bounty strategy

Today, TX Group's SecDevOps teams work autonomously using agile methods to develop new digital products — which, in the hyper-competitive world of media, change constantly.

This mandated a new approach to product security: the replacement of traditional audits (which, by definition, only produce a point-in-time snapshot) to continuous monitoring of assets and systems. Annual audits at the group's digital companies, vulnerability scanning of legacy solutions run on-premises in their own data center, and a managed SOC… these have all been superseded.

For all TX Group's free and paid media (including *20 Minuten* and *Tamedia*), for its digital marketplaces and for new companies (TX Ventures), audits have been changed into bug bounty programs, while vulnerability scanning is performed by web app scanning tools. When vulnerabilities are detected, they are submitted via API to TX Group's Bugcrowd-managed bug bounty program.

> "If a company says it's running a bug bounty program, then every security researcher and hacker already knows that the company has already done a lot of security work and has an entire security environment in place. A bug bounty program is one of the last measures in the chain, and it's an indicator of how well a company manages its security."
>
> - Olivier Martinet,
> Group CISO, TX Group



Why Bugcrowd was chosen

TX Group chose Bugcrowd after considering proposals from several major bug bounty solution providers, including Bugcrowd, HackerOne, YesWeHack, and Synack.

Proposals were evaluated according to: a cost-benefit analysis (price), availability of a managed platform, availability of a variety of out-of-a-box integration options (e.g. Slack, Jira etc.) and — most importantly — the ability to provide the Group's SecDevOps team with a customized tool.

Outcomes

TX Group's managed bug bounty program has delivered spectacular results. Despite the company conducting initial audits before commencing programs, **up to 10 times more vulnerabilities were discovered — even 20 times more in some cases; and a significant number of vulnerabilities were designated as critical.**

This initial rush of discovery inevitably meant that program costs were initially higher than expected. However, as of April 2022, no critical vulnerability has been detected for more than six months. Which means that TX Group assets are currently very secure, and that they now need to only pay for the use of the platform since no rewards are being paid. By way of comparison, Olivier Martinet points out, a classic audit always incurs costs whether vulnerabilities are found or not.

> "Integration options for developers were the deciding factor, not the price. With other providers, you can pull things out via API. With Bugcrowd, we simply already had a ready-made Slack-Jira integration. And those are the two that are important to us. We don't have to develop it, it's just already there and it's used a lot."
>
> - Olivier Martinet,
> Group CISO, TX Group

The Bugcrowd Advantage

More High Value Vulnerabilities

Many researchers focusing on their own area of expertise

Lower Cost Per Vulnerability

Competitive pay-per-bug means clear ROI faster

The Right Crowd At The Right Time

CrowdMatch™ finds the right testers for continuous coverage

Faster Fixes

Close gaps with workflow automation and SDLC integration