CYCOGNITO

CASE STUDY: MEDIA AND ADVERTISING

Ströer Uncovers, Secures Hidden Digital Assets with CyCognito

German media house gains global external attack surface and risk visibility

Key Results

- Gained continuous visibility into complete external attack surface for the first time (~40,000 assets), including subsidiaries and joint ventures
- Discovered previously hidden vulnerabilities, which improved the company's security posture, and helped the company avoid excessive pen tests
- Reduced external attack surface footprint by shutting down shadow servers and unmanaged websites
- Enabled >50 subsidiaries to perform independent monitoring with the centralized CyCognito platform, reducing remediation time
- Gained comprehensive reporting used to inform the Board of Directors of subsidiary risk levels and improvements

Story

When Benjamin Bachmann joined the German media company Ströer two years ago as the Vice President Group Information Security, the company didn't have a good map of its external-facing digital assets. Part of the reason is because of its vast operation, which includes more than 100 subsidiary companies operating in different sectors, each with its own IT department.

"At first we didn't even know how many digital assets we had," Bachmann says. "When I started, no one monitored that. It was just a guesstimate."

That's not surprising considering the extensive portfolio of Ströer. With revenues of 1.77 billion euros, Ströer continues to grow despite the global advertising market's decline.

STRÖER

CUSTOMER PROFILE

Ströer is one of the leading German media companies and is listed on the MDAX of the German Stock Exchange. The company has more than 100 companies that employ 10,000 people in more than 100 locations.

Ströer's vast enterprise includes outdoor advertising, digital media, and dialogue marketing as well as e-commerce and digital as a service (DaaS). In addition to owning the largest news portal in Germany, it also operates stats provider Statista, call centers, and a cosmetic company, among others.

In the past eight years alone, Ströer acquired Germany's biggest Internet service provider T-Online's online portal, and in two transactions acquired Statista. It also added Classmate's German version called StayFriends, acquiring the firm from United Online, the parent of Classmates.com. As their digital presence grew, so did their attack surface.

> **My key takeaway would be to care about your internet-facing assets, your attack surface because even if you think it's not important to know about that yet, the adversaries will know about your attack surface, and they don't care if they hack you or someone else."**
>
> **Benjamin Bachmann**
> Vice President, Group Information Security

Ströer had previously sought to map its external assets. The company hired a consultant and planned to conduct vulnerability scans to map out their external attack surface. But executives pulled the plug after 15 months when it became apparent the approach wasn't working as intended.

"This resulted in 50 or 60 Excel files without any connection between them," Bachmann says. "There was no way to calculate risk. While the initiative was of some value, it didn't meet our expectations considering what we spent."

Solution

Reconnaissance with Proactive Remediation

After the failed project, the Ströer security team launched a search for a comprehensive external attack surface solution to identify and remediate security risks, from hidden attack vectors to misconfigured assets. After reviewing several external attack management tools, Ströer chose the CyCognito platform.

None of the other external attack surface solutions they reviewed were able to replicate Ströer's structure successfully.

The CyCognito platform uses machine learning, natural language processing, and a graph data model to discover and relate all business relationships in your enterprise, including those of acquisitions, joint ventures, and cloud environments. From this reconnaissance, it creates an asset inventory autonomously, identifies blind spots, offers remediation, and then continuously monitors your external environment to help you proactively shut down potential points of attack.

"It was pretty easy for us to decide on CyCognito because what's outstanding from my point of view is that you can build up your team's hierarchical structure and company portfolio. You can assign different assets to Company A and others to Company B. All of our companies can work within one platform with robust access controls," Bachmann says.

His security team liked CyCognito's friendly user interface and easy-to-use search function, which made onboarding simple and quick.

"It's really nice that you have some really huge search capabilities so you don't have to learn any new language or click 1,000 times to navigate," he says.

Implementation

Despite Ströer's complex and vast organizational structure, implementation was very fast and easy. "It took us six weeks to be really productive, but we could start with some of the businesses after about a week," Bachmann says.

One of its larger hurdles was determining exactly what assets it owned and didn't own as part of its acquisition of T-online, the largest German news portal. "It was just a mess to get all the false positives out of that," says Bachmann.

Benefits

Uncovered Hidden Assets

With CyCognito running "we saw immediately that we have more assets than we thought we had. And we saw a lot of vulnerabilities we remediated," Bachmann says.

Within a few weeks, they had winnowed and remediated many of the vulnerabilities and saw those numbers decline.

"What was really interesting was to see the amount of cross-site scripting and other web application vulnerabilities we had in websites we own that have not been used by attackers as far as we know," he says. "And those have been fixed."

The security team monitors some 40,000 assets in CyCognito, Bachmann says. In addition to Internet sites, they have some assets running through cloud providers Amazon Web Servies, Microsoft Azure, and Google Cloud Platform.

Ströer is running the platform for its subsidiaries as a managed service at a high level and then 50 or so subsidiaries at any one time use CyCognito to police their own digital assets. "Everyone in the company is positive about CyCognito and is interested in having a good risk level," Bachmann says.

CyCognito: A Game Changer

"This is the game changer because I don't have to call every time I see an unpatched server," he adds. "I can just tell that company 'It's your part of the game to take care of your assets.'"

Within the first six months of running CyCognito, Ströer mitigated a number of vulnerabilities. "Most companies had some shadow servers that no one was administering anymore," he says. "It was quite nice to see them from the outside and take action. We shut down some websites as well."

Although Ströer has seen the number of hidden vulnerabilities cut in half when new companies are acquired, new services are launched or a product or company is integrated, Bachmann has noticed an increase in the company's digital footprint. But he can quickly spot that trend and take corrective action.

"On my end, we save a lot of time because I can just click into the platform and tell one of the companies 'your Internet footprint is larger," he says. "And our subsidiaries probably save time as well because CyCognito delivers quite nice instructions on how to fix vulnerabilities, for instance, or how to validate if it's really there."

> **CyCognito is worth every cent we pay and it helps me sleep better because I know we're checking our internet-facing assets on a regular basis."**
>
> **Benjamin Bachmann**
> Vice President, Group Information Security

Discovering hidden vulnerabilities improved the company's security posture, and helped the company avoid additional costly penetration tests (pen tests). "We cannot afford to pen test every website we own every few weeks or months," Bachmann says.

Additionally, pen testing reveals just a snapshot in time, he says. "CyCognito helped us a lot because we have a really good continuous understanding of what our defense looks like."

Don't Rely on Security Snapshots

Bachmann urges CISOs not to rest on their laurels and rely on their "known" attack surface or periodic manual testing but to act proactively by investing in a platform that automatically and continually scans their attack surface for vulnerabilities of known and unknown assets.

Doing so could help companies react faster to breaches and can save companies hundreds of thousands of dollars. "If one of the assets I don't know about has a breach, I'm probably not able to react fast enough and then I can be in severe trouble," Bachmann says.

To learn how the CyCognito platform uniquely helps you identify and prioritize the paths of least resistance into your IT ecosystem, so that you can eliminate them, visit **cycognito.com**.

CYCOGNITO