Scirge Case Study

-Takeaways by you, for you.

Kovárczi Béla- Head of IT Security Systems Operations
Szerencsejáték Zrt.

What problems and risks did Szerencsejáték Zrt. face regarding Shadow IT?

The main risks of Shadow IT include potential data leaks, unregulated or weak access controls, and, in some cases, licensing issues. In many instances, employees did not know why a registration occurred on a particular website, highlighting the need for deeper awareness.

Additionally, at Szerencsejáték Zrt., nearly half of the online accounts created with corporate email addresses were not related to work tasks and therefore needed to be deleted.

What methods were previously used to address this, and how did Scirge help?

Previously, the company relied on firewall and security logs, as well as information discovered during daily work, to try to identify unauthorized usage. However, this approach proved extremely time-consuming and left many blind spots. Although regulations and training were already in place, Shadow IT detection was still not sufficiently effective.

The introduction of Scirge marked a breakthrough by providing complete transparency regarding the use of web applications associated with corporate email addresses. As a result, even smaller, less-known services that had previously gone unnoticed could be identified. The system allowed department leaders to review which applications were truly necessary and which posed unnecessary risks.

Additionally, it provided immediate feedback to users engaging in risky behavior, such as password reuse, greatly supporting rapid response and awareness.

What were the key results achieved with Scirge?

The company achieved tangible results in a short period. Highly accurate information about applications and users allowed for significant reduction of Shadow IT and the elimination of unnecessary registrations and online accounts.

Password hygiene also improved significantly, with 58% of users updating their passwords in response to Scirge alerts.

The implementation of the system also initiated entirely new processes, such as reviewing accounts of departing employees and establishing protocols for handling identity misuse and inactive accounts of former employees.

How difficult was the system implementation, and would you recommend it to other organizations?

Installing Scirge required only two person-days, and the deployment of browser extensions proceeded smoothly. According to Szerencsejáték Zrt.'s experience, the system provides a level of transparency that was previously unimaginable, and it is therefore strongly recommended for other companies.

SZERENCSEJÁTÉK ZRT.

SCIRGE
SHEDDING LIGHT ON SHADOW IT