SWAN

SECURING WEB APPLI-CATIONS

The digitalization of business has brought companies new opportunities, but also new risks. Web portals, customer zones, and online applications are now key tools for communicating with customers, while at the same time becoming some of the most frequent targets of cyberattacks.

MILAN DZILSKÝ
Commercial Director
at SWAN

Milan Dzilský studied Information Systems Management at the Faculty of Management of Comenius University in Bratislava. He has worked in the telecommunications sector, with a short break, since 2003. He began his career as a hardware product manager at Eurotel Bratislava (later T-Mobile Slovakia). He later served as Country Manager for Slovakia for Sony Ericsson (later Sony Mobile) and subsequently for Xiaomi. As part of the CEE team, he helped build awareness of a new brand in the market. He was responsible for strategic development, business results, and managing marketing activities for both B2C and B2B segments. He later worked as Commercial and Marketing Director for the Czech hat manufacturer TONAK. Milan Dzilský has been serving as Commercial Director for Corporate Customers and ICT since October 1, 2024.

We spoke with Milan Dzilský, Commercial Director at SWAN, about how companies can protect themselves and why protecting web applications is becoming increasingly important.

Cybersecurity is often discussed today. Why is it so important?
Digital technologies now form the backbone of how most companies operate. Whether it is an e-shop, a customer portal, or internal applications, everything is accessible online. This means companies are exposed to various types of cyberattacks.

Attackers try to obtain sensitive data, disrupt the operation of services, or damage a company's reputation. That is why cybersecurity is becoming a strategic issue that goes beyond the boundaries of the IT department.

What do attackers focus on most often?
One of the most common targets is web applications and online portals. These often contain login credentials, personal data, or business information.

Attackers use various techniques, such as DDoS attacks, which can take a website offline, or attempts to exploit security vulnerabilities in applications. Automated bot attacks are also common, where bots try thousands of combinations of login credentials. For companies, this can mean not only a technical problem but also a loss of customer trust.

Many companies use firewalls. Why is that no longer enough today?
A traditional firewall primarily protects the network infrastructure. However, modern cyberattacks often target web applications directly and the communication between the user and the server.

> **Digital technologies now form the backbone of how most companies operate.**

This is why specialized security solutions have emerged that can analyze web communication in real time and identify suspicious behavior before an attack even reaches the system. It represents a far more advanced approach to protecting digital services.

How does SWAN respond to these threats?
At SWAN, we have long been focusing on cybersecurity solutions for companies. One of these solutions is the Web Application Protection (WAP) service, which acts as a digital shield for websites, portals, and online applications.

This system monitors all communication directed to a website or application and can identify malicious requests before they reach the application itself. In practice, this means potential attacks are stopped before they can cause any damage. The solution is suitable for various types of services, ranging from corporate websites and e-shops to customer portals or internal applications accessible from the internet.

What types of attacks can such protection detect?
Modern security systems can identify a wide range of attacks. These include attempts to exploit vulnerabilities in web applications, SQL injection, XSS attacks, or automated bot attacks. They can also filter malicious traffic and help protect applications against DDoS attacks or brute-force login attempts. Importantly, the protection works continuously and analyzes communication in real time.

Why are companies increasingly using such solutions as a service?
Cybersecurity is a dynamic field. New threats emerge practically every day, and companies must respond quickly.

However, building an in-house security team and infrastructure is financially and organizationally demanding for many companies. That is why the security-as-a-service model is becoming increasingly popular.

Companies gain modern protection without the need to invest in their own hardware or large security teams. At the same time, they benefit from technological solutions that are continuously updated in response to evolving threats.

How should companies approach cybersecurity in the future?
The most important factor is a proactive approach. Companies should not address security only after an incident occurs, but already at the stage of designing their digital services. This means regularly analyzing risks, updating systems, and implementing solutions that can protect both web applications and data communication.

> **Companies should not address security only after an incident occurs, but already at the stage of designing their digital services.**

Digitalization will continue to grow in the coming years, and with it the number of cyber threats. Organizations that consider security early on will have a significant advantage, not only in terms of protecting data but also in maintaining the trust of their customers.