The Automated Security Audit Platform for MSPs.

lywand software

Why Regular Audits are Crucial

Automated attacks, digitization, and the increasing complexity of IT infrastructures make it increasingly difficult to maintain an overview of the IT security situation. The attack surface grows daily, and the lack of visibility into the IT security status poses risks. A single security vulnerability may be enough for a hacker to infiltrate a system unnoticed.

The Features in Detail

With lywand, you can conduct comprehensive security assessments from the perspective of a potential attacker for your clients:

- The external infrastructure, including (sub)domains, email addresses, and IP addresses, is analyzed for vulnerabilities. Additionally, it is checked whether stolen company data appears on the dark web.
- The internal infrastructure, such as laptops and servers, is checked daily for known security vulnerabilities, best practice configurations, and current patch statuses. Basic security mechanisms like the Windows Firewall and antivirus software are also monitored.
- The network check analyzes all devices in the internal network (such as printers, smartphones, and other IoT devices). This quickly identifies where vulnerabilities and configuration errors are hidden – or where necessary system hardening is lacking.

After a security audit, the security situation of your clients is presented clearly. Based on the results, lywand provides specific recommendations for addressing the vulnerabilities.

During the next security audit, lywand checks whether the measures were successful and whether the security gaps have been closed. The results are summarized concisely and understandably for your clients in a management report.

Data Storage

Lywand stores all data encrypted in the database. The following is collected for regular operation:

- Your personal data as well as customer data provided during registration
- Identified IT infrastructures & security vulnerabilities
- Recommended measures to address these security vulnerabilities

Provision of Infrastructure

To make IT security easily and cost-effectively accessible to everyone, the environment runs in the next layer data center in Vienna (Austria).

This is secured both physically and digitally and certified according to established IT standards (ISO-27001, Code of Conduct for Internet Service Providers, ANKÖ LgU Seal, Bundesbeschaffung GmbH Partner, Cyber Trust Austria Silver Label). Details can be accessed **here**.