How secure are your payment transactions?

Security check against cybercrime

www.slg.co.at

Professional analysis & security assessment

Fraud cases in payment transactions are on the rise, thanks to – and not despite – increasing automation and digital networking.

We analyze your payment processes and test their security in a simulated emergency.

With the increasing instances of fraud and cyber attacks in treasury departments, ensuring the security of payment transactions has become more crucial than ever.

Having clear and traceable processes is a must for secure payment transactions – and that's exactly what we focus on. Our experience has shown that technical security is often a key factor. We investigate both processes and infrastructure from the perspective of a seasoned treasury consultant and an IT security expert to make sure your defenses are strong.

- Are processes consistently built to be safe and auditable?
- Do the current processes provide opportunities for manipulation by employees or external attackers?
- How well-protected are system interfaces against external attacks?
- How vulnerable is the corporate environment to phishing or social engineering attacks?

The SLG Security Check

Approach and project methodology

To offer you a comprehensive project framework seamlessly, we've partnered with a renowned IT expert: Hackner Security Intelligence specializes in conducting high-quality technical security assessments.

This collaboration brings together decades of experience in cash management with essential IT expertise. This not only positions us a step ahead of our competitors but also ahead of those seeking to exploit security vulnerabilities.

In conjunction with Hackner Security Intelligence, we have defined a series of 'Penetration Tests' tailored to the specific nuances of your system infrastructure and the orientation of your treasury function. This ensures a targeted and effective assessment of your security landscape.

Deriving insights from results and follow-up measures

Based on the test results, we document identified vulnerabilities in a results report and provide specific points for improvement, prioritized in a list. These may include system-related steps (such as encrypting payment files) as well as concrete training measures for employees. Sensitization, given the increasingly creative nature of fraud cases, is a crucial success factor. The motto is: 'Fake President was just the beginning!'

Identifying attack points and implementing countermeasures

Understanding how fraudsters penetrate the financial flow of companies

Analogous Attacks
- Invoice manipulation
- Signature forgery
- False bank transfer
- ...

Social attacks
- Phishing
- Social engineering
- Blackmail
- ...

Digital Attacks
- Malware
- DDoS
- Hacking
- ...