Does cyber security consulting also make sense for outsourced IT?

Author: Peter Monien

In an increasingly digitalized world, companies often rely on external service providers to reduce costs and focus on their core business. When outsourcing their IT to service providers, companies often assume that the contract also fully covers the issue of security. Read this article to find out why this is a mistake and what risks companies face as a result.

The problem with security in outsourcing

Clients often implicitly assume that IT security is fully covered by the service provider. This is not correct:

Cybersecurity cannot be 100% outsourced to service providers

- Professional external IT service providers with good security know-how set up individual IT systems securely and keep them up to date (patch management).
- The budget of IT service providers is often geared towards the one-off installation and ongoing operation. An active search for cross-system vulnerabilities, especially after major IT changes or new system releases, does not take place. A regular vulnerability scan is no substitute for a penetration test (see article).
- Those who monitor themselves tend to overlook errors or view risks less critically. This also applies to IT service providers who check the systems they set up and maintain themselves.
- IT service providers traditionally do not advise customers in the areas of organization, processes and security awareness culture, which are also important for cyber security.
- Cyber security is a management task. As there is no such thing as 100% security, trade-offs must be weighed up. If the client is not actively involved and controls the suppliers involved, the resources will be used according to the service provider's standard. However, this approach is not necessarily optimal for the business and the efficient reduction of the associated risks.

Even IT is not completely secure: insidious errors and security gaps

- Suboptimal organizational measures and processes lead to a suboptimal security maturity and offer hackers an unnecessarily large number of attack vectors despite well-secured IT.
- Even with careful IT support, errors can creep in over time. Configuration changes, software updates or new systems always harbor risks.

- An external cyber security consultant identifies these IT vulnerabilities through penetration tests that combine automated scans with human experience and intelligence. In this way, potential attack vectors can be closed before any damage is done.
- From practical experience, we know that security risks tend to accumulate over the course of a partnership with an IT service provider. A sporadic external test can prevent this.

Forensics: A special field for emergencies:

- In the event of a cyber attack, quick and precise action is crucial. This is where digital forensics and specialist security knowledge come into play.
- The external IT service provider is the key external player when it comes to a cyber incident. For example, they restore systems from backups and reinstall systems. However, incident responders have the specialized knowledge and equipment to secure digital evidence, analyze attacks and identify perpetrators. This specific expertise usually goes far beyond the capabilities of a regular IT service provider.

Conclusion

Professionally outsourced IT is advantageous, but it does not replace all the necessary cyber security measures. Achieving a high level of cyber security maturity is not just about systems, but also about an organization's processes and employees. In addition, the client must be actively involved in the process in order to achieve a resource-optimized reduction of the risks associated with their business.

Independent external experts can also advise on topics that go beyond IT. They bring a neutral and objective perspective to the assessment of IT security, uncover blind spots,and thus offer an indispensable additional layer of security. Especially after significant IT changes, a review of the systems by a specialist should be considered.

Do you have any questions or need support in optimizing your cybersecurity? We look forward to hearing from you.