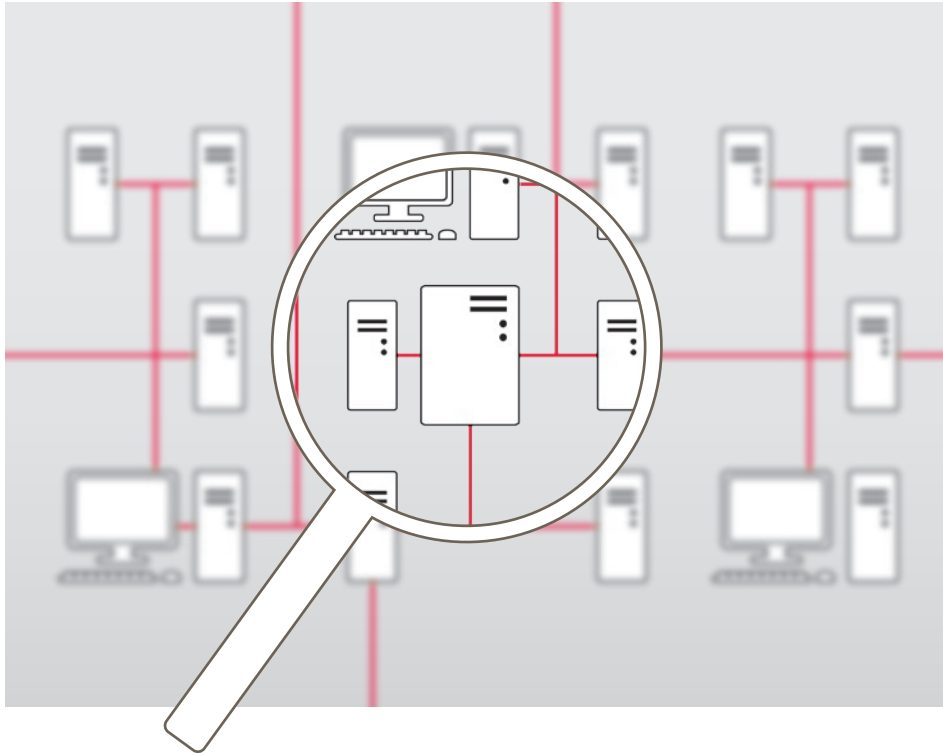


Checking Existing Security Infrastructures – How Secure Are They?



Benefits:

- » Disclosure of vulnerabilities in your IT infrastructure
- » Practical implementation of the IT security concepts you have
- » Protection of your company values

Security requirements now need to be considered as a necessary part of any IT project. But how effective are the implemented measures really? The results of a security audit indicate where action is absolutely critical, how measures and investments can be meaningfully prioritised, what security level has already been achieved and what remaining risks are to be reckoned with.

■ Point of action: firewall

If your firewall systems are configured properly, you should be able to successfully prevent most potential web-based attacks. But firewalls are unable to protect against all attacks for reasons inherent in the system. It must be possible to access an available web server despite the firewall. Specific attacks targeting web servers can pass through the firewall and have to be fought by other means. Using so-called zero-knowledge penetration, our experts identify points in your systems which are vulnerable from the Internet, without any specific knowledge of your IT.

■ Point of action: mobile access to your network

Although increasing numbers of companies provide external access for staff via virtual private networks (VPNs) and the Internet, it is still

possible to find dial-up facilities via the phone network, in particular for maintenance access by manufacturers. An automated analysis of extensions, VPN gateways and mobile end devices indicates which services are available and what the corresponding security mechanisms look like.

■ Point of action: web portal

Communicating with customers via web servers is particularly prone to attacks. Using so-called cross-site scripting, attackers are able to gain unauthorised access to servers. SQL injection attacks enable the export of entire databases via web interfaces. In this type of situation our experts can help with the detection and removal of such threats.

■ Point of action: your own network

The bigger the organisation and the internal network, the greater the likelihood of an attack originating in your own network – whether this is by your own staff, by external personnel with access to the network or by the infiltration of malware which is active on a PC in the network without the knowledge of the staff. Therefore, the internal network must also be considered in a security analysis.

■ Point of action: people

If attackers make no headway with your IT systems, they may turn to your staff for information about your network. This method is referred to as social engineering. Attackers assume a false identity and attempt to induce staff to divulge sensitive information such as passwords or unknowingly introduce malware into the company network via complimentary CDs. The global spread of phishing attacks in the online banking sector shows how effective these methods can be.

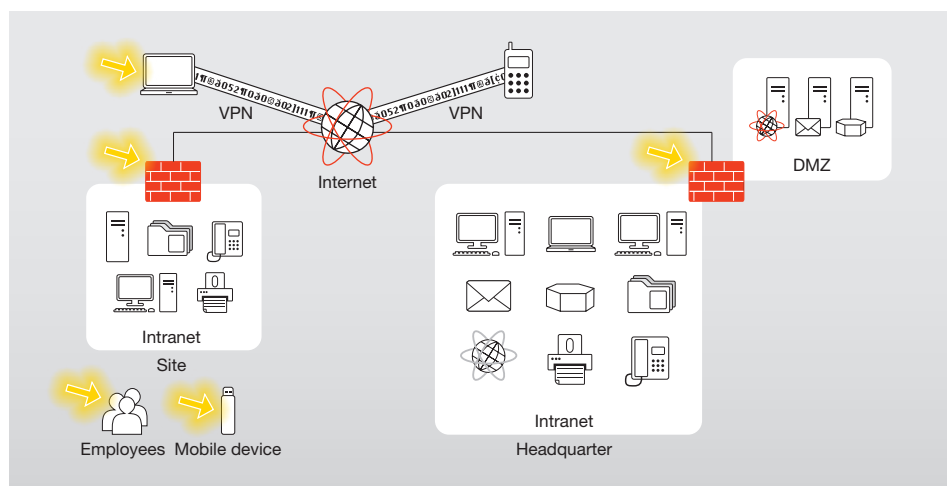
Can your IT security measures withstand an attack?

Audits

Procedures, processes and directives are just as important as technical systems when it comes to security. Are your security-relevant application areas adequately regulated? Are necessary measures such as role separation or a double-checking principle realised in processes? Are your security measures regularly checked and developed further with the technology? We check the IT security processes you have already established and process documentation for completeness and topicality and ensure that your security concepts are actually implemented as opposed to collecting dust on the shelf.

Evaluation

For our analyses, we rely not only on the results of automatic scanners and tools, but also put our many years of experience to use. Consequently, we can concentrate on the most important risks and recommend strategic action. Our analyses and documentations follow the standard OSSTMM (Open Source Security Testing Methodology Manual). Thus, we ensure a comparability of the results.



- ➔ Preferred points of attack
- Firewall
 - Mobile access to your network
 - Web portal
 - Your own network
 - People

secunet is your experienced partner

Having completed more than one hundred security analysis projects focusing on various aspects, our experts have gained an enormous wealth of experience in carrying out security audits. They are therefore able to disclose and analyse critical weak points in a target-orientated way. We have performed extensive audits in large organisations which comprised the big picture of IT security, from the technical system configuration to security processes and emergency planning.

By comparing your security structures against best practices, we can provide valuable information on optimising security and operations, prevent damages and thus reduce costs.

More information:
www.secunet.com/en/pentest



secunet Security Networks AG
 Kronprinzenstraße 30
 45128 Essen, Germany
 Phone: +49-201-5454-0
 Fax: +49-201-5454-1000
 E-mail: info@secunet.com
www.secunet.com