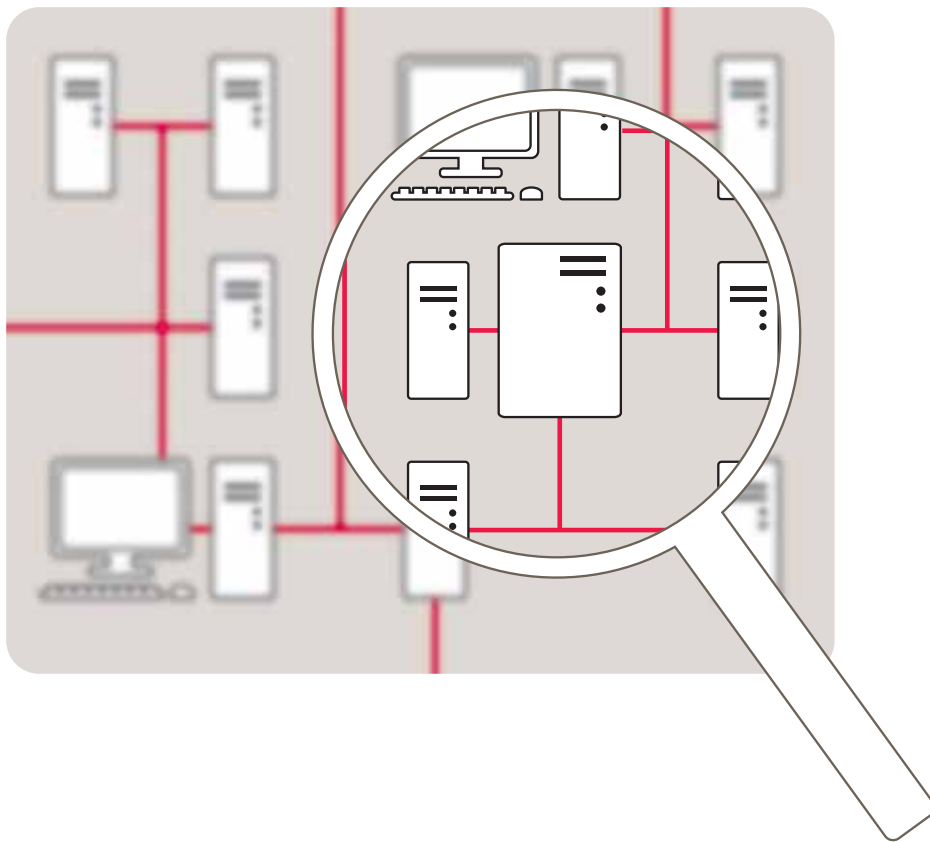


**secunet**

## Analysis and Audits

# Checking existing security infrastructures – how secure are they?



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

### Is the firewall attack-proof?

If your firewall systems are configured properly, you should be able to successfully prevent most potential attacks from the web. But even firewalls may have vulnerable points and it is important to also configure the internal servers themselves for the utmost security.

Using so-called zero-knowledge penetration, our experts attempt to identify vulnerable points in your systems from the Internet, without any specific knowledge of your IT. In addition, the “tightness” of the firewall systems at the transition point between the DMZ and the internal network can be determined by means of so-called perimeter penetration.

### Your advantages:

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

### 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.

### Weak points as a result of WLAN

Wireless local area networks (WLANs) are practically ubiquitous. But it is often overlooked that the range of wireless transmission extends beyond the premises. This gives unauthorised persons the opportunity to access the WLAN and read or manipulate data. Consequently, our experts also analyse your WLAN configuration and provide information on weak points and appropriate 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 their extensions as well as analysis of the security of mobile end devices indicates which services are available and what the corresponding security mechanisms look like.

### The human factor

If an attacker does not find an entry point into your IT systems, he can still ask your staff for assistance. Such attacks, known as social engineering, involve the use of a false identity in an attempt to throw staff off their guard and get them to divulge sensitive information such as passwords, or to support the attack in other ways. The global spread of phishing attacks in the online banking sector shows the success which can be achieved through such methods.

### secunet Security Networks AG

IT security and its trend-setting usage is the core competence of secunet Security Networks AG. The development and implementation of IT security solutions for sensitive data turn secunet into a specialist in great demand. Excellent technological understanding is reflected in our consulting services and modulated products. Progressive digitalization of processes and communication channels of all kind pose new challenges for secunet day-to-day. Due to our large know-how we set standards in the IT security market. Our extensive clientele comprises national and international companies and affiliated groups as well as the public sector. About 230 highly qualified and experienced employees at seven branch offices in Germany as well as at further offices in subsidiaries in Switzerland and the Czech Republic are engaged in the creation of innovations, the optimal settlement of projects and our twenty-four-seven support.

### Can your IT security measures withstand an attack?

#### Audits

Procedures, processes and directives are at least 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 also check the security documentation you have available for completeness and topicality. We ensure that your existing security concepts are put into practice instead of collecting dust as “shelfware”.

#### Evaluation

For our analysis, we do not only rely on the results of automatic scanners and tools, but also just as much on our many years of experience. As a result, we can concentrate on the most important risks and recommend strategic action.

### secunet as 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 very 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.

Editor:

# secunet

secunet Security Networks AG  
Kronprinzenstraße 30  
45128 Essen, Germany  
Phone: +49 - 201 - 54 54 - 0  
Fax: +49 - 201 - 54 54 - 123  
E-mail: [info@secunet.com](mailto:info@secunet.com)  
[www.secunet.com](http://www.secunet.com)