InfoGuard
SWISS CYBER SECURITY

PENETRATION TESTING AND ETHICAL HACKING

Your technical security systems under scrutiny.

PENETRATION TESTING – TARGETED, PRECISE, PROVEN AND HELPFUL.

Reducing risk, taking account of legal provisions and worrying about image are the reasons most frequently cited when investment in information security is under discussion. But information security is a great deal more than just avoiding serious shortcomings. It is a precondition for using present day technologies reliably and easily in order to enhance the reputation of the company.

In conducting a penetration test our security experts simulate a real attack. This will show whether the infrastructure is sufficiently protected against hacking from outside and inside and whether it is compatible with the accepted residual risks.

The aim of penetration tests is to review IT security. The attack is controlled in such a way that any weaknesses, reflecting the reality as far as possible, are identified. The scope of the systems being tested ranges from network services and online shops, complex corporate networks up to the users of the infrastructure.

In order to test these overriding factors in detail we offer modular penetration tests. They range from the passive gathering of information, targeted external penetration tests from the internet to identifying vulnerabilities that can only be identified on site. Our approach is orientated towards the acknowledged OWASP, OSSTMM and ISO 27001 standards and methods.

Our services include:

- Identifies potential weaknesses in your security concepts, systems and applications.
- Analyses the IT infrastructure and evaluates the protective measures that are in place.
- Increases the integrity, confidentiality and availability of data, applications and systems thanks to tried and tested security measures.
- Provides assistance in fulfilling legal provi-sions and other compliance requirements.

1 Planning the attack scenarios

As a rule, the penetration test is undertaken in several steps. Firstly, the aims of the review need to be defined and the use of the chosen technologies and methods coordinated. The kick-off meeting is followed by a detailed threat analysis. This gives us an initial idea of the existing topology, in other words the infrastructure, systems and applications, without infiltrating the identified systems (black-box approach).

Based on the results of this first phase the planned attack scenarios are then discussed and defined together with the customer. The result is an individual penetration test, which takes full account of the threats posed to the customer.

The infrastructure is then examined using the agreed types of attack. This will shed light on whether the company network is sufficiently protected against targeted attacks. During this test run the shortcomings identified are exploited to attack further systems and thus penetrate deeper into the network. Should our specialists identify critical gaps in security they are immediately reported and dealt with as a matter of urgency. In conjunction with our penetration tests we employ a number of different attack techniques.

2 Attack techniques

Infrastructure tests

To simulate a concrete attack we use a variety of manual tests. Our team attempts to take advantage of identified weaknesses in the infrastructure to obtain unauthorised access to the network or individual computers. In doing so we examine:

- remote access (RAS or VPN access)
- the server infrastructure (domain controller, DNS server, terminal server, etc.)
- the malware filter for email transmission and access to the internet.

We undertake the penetration tests both internally and externally. And we also investigate how the security systems have been configured and implemented.

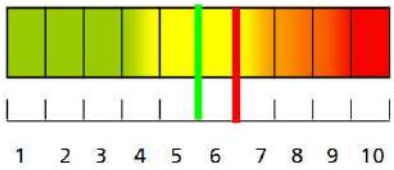
Web application tests

For web hacking we focus on weaknesses in web applications such as cross-site scripting or SQL injection, but also on (logical) errors in authentication, authorisation or session handling. Depending upon the situation the analysis is undertaken with a total of 25,000 different automated and manual single tests.

User behaviour

In order to circumvent the security systems we apply social engineering methods. These examine the security awareness and actions of the employees. Using phishing mails and drive-by infections, or inside-out attacks, for example, we attempt to obtain sensitive information or passwords.

3 Results of the analysis and test report



On conclusion the customer is presented with a comprehensive test report. This ensures that the results are presented in order of priority and can be easily understood. The report also includes the detailed process and the findings of the penetration test. Each weakness identified is accompanied by detailed documentation describing the security gap and how this can be exploited. In addition, a special risk analysis is drawn up that sets out the potential dangers of the vulnerabilities in the overall context of the company network.

Finally, constructive solution proposals for the individual weaknesses are presented as a means of directly optimising security. Depending upon the operating systems and applications being used general checklists to increase security are also handed over. In a concluding workshop the test report is discussed with the customer and the next steps agreed.

We have proven specialists for information security who are able to demonstrate many years experience in the localisation and testing of shortcomings in applications, systems, networks and configurations. Due to continuous changes in the IT landscape new vulnerabilities are identified almost every month. Thus, in order to mount a realistic attack, our penetration tests always take account of the latest technologies. Our wide-ranging technical expertise in operating systems, security systems, applications and databases is at your disposal and can be drawn upon in the form of additional services.

INFOGUARD – YOUR CERTIFIED PARTNER FOR REVIEWING TECHNICAL SECURITY

Your business processes can only function properly if the correct information is in the right place at the right time. Confidentiality, integrity and availability of the information play an overriding role.

InfoGuard provides an independent assessment of your information security. We show you which organisational, technical and personnel weaknesses are manifest in your company and how you can counteract these.

Our services embrace the following domains:

- Security Audit based on ISO 27001/27002
- GAP analysis in terms of ISO 27001 certification
- System and architecture review
- Penetration test based on OSSTMM
- Vulnerability scan
- Social Engineering Audit

Your security is our goal –
we analyse and optimise your security system!

InfoGuard – The Swiss Cyber Security Expert

InfoGuard is the Swiss expert for comprehensive cyber security and innovative network solutions. You can benefit from our experience, professionalism and reliability in the auditing, consultation, architecture and integration of leading network and security solutions. We deliver state-of-the-art cloud, managed and cyber defence services from our ISO 27001-certified InfoGuard Cyber Defence Center located in Switzerland.

InfoGuard AG
Lindenstrasse 10
6340 Baar / Switzerland
Phone +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern / Switzerland
Phone +41 31 556 19 00

INFOGUARD.CH