Penetration Testing

AEC

Check out the security level of your systems and applications before someone else does!

Penetration testing simulating a hacker attack performed both on the network, as well as on the application level, will evaluate whether your systems are able to resist a real cyberattack from the outside environment, including their ability to resist any unauthorized interventions performed by the employees, whether executed deliberately, or because of human error.

Penetration testing will help you to detect any deficiencies occurring in the system design and architecture, including identification of any inadequately sized performance-related system components.

Penetration testing will check the level of security when it comes to confidentiality, integrity, and accessibility of data processed by electronic systems and thus will provide a trouble-free operation of the ICT organization and the related business processes.

Services offered

Infrastructure penetration testing

Detailed security screening of all the company computer network components accessible either from the Internet network or through the internal company network. We will probe the organization from the attacker's point of view; either as an attacker who only has publicly available information at his disposal, or as someone who already has access to the internal organization systems in order to simulate an internal user or malware.

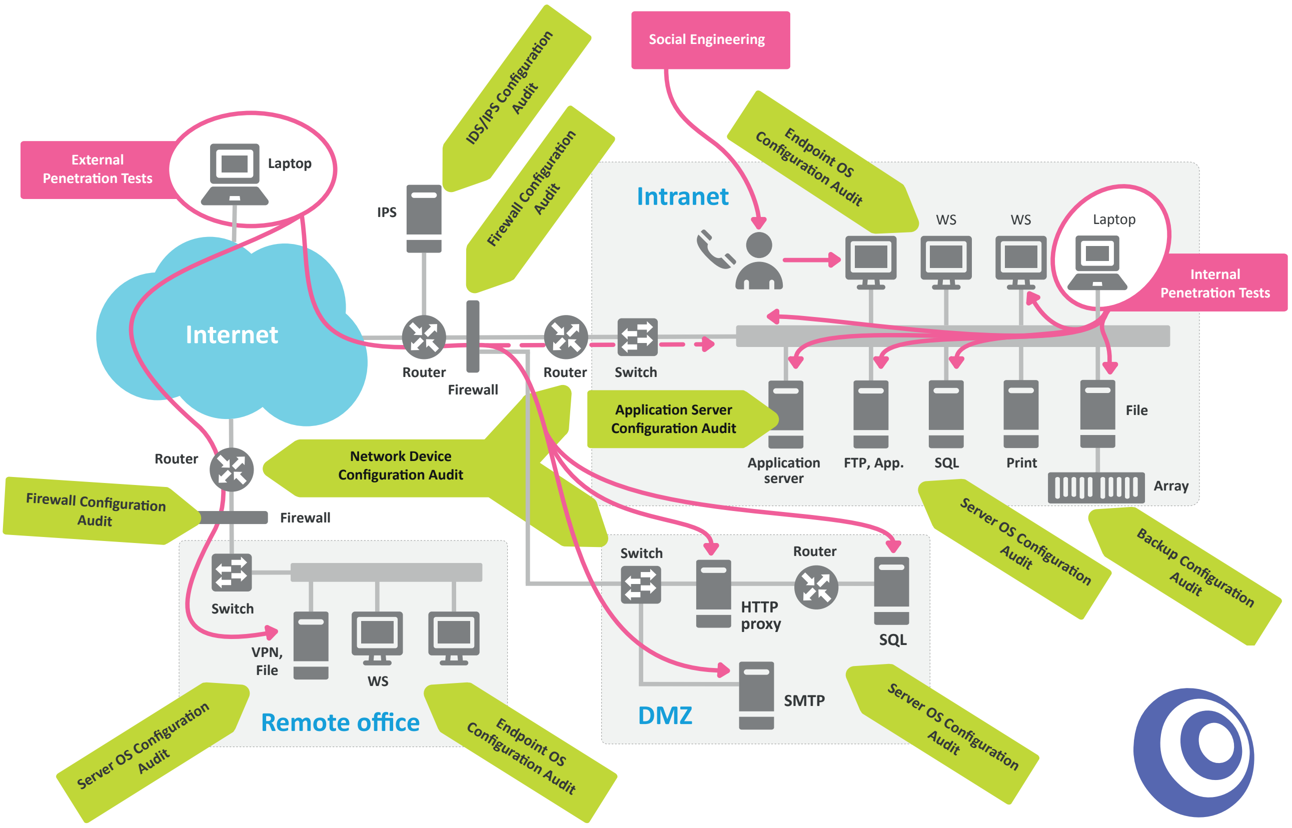
Application penetration testing

We are providing application security screenings, from simple static portals, up to complex web applications and services with advanced business logic.

We have vast experience with testing of native mobile applications for the Android and iOS platforms. Desktop applications of the "thick client" type that are often neglected when it comes to security are our specialty. Apart from the indispensable automated testing, we mainly concentrate on the manual testing, which includes complex communication technology links and application business logic.

Our solution

- More than 25 years of experience in the area of security in Central Europe.
- Broad team of 15 certified specialists with experience from hundreds of performed penetration tests of critical applications and extensive systems.
- We put emphasis on importance of manual approach to the testing, which results in discovering a greater number of bugs, especially in the application business logic.
- Evaluation of the company ICT security level and definition of real risks in the context of presumed impact to business.



Social Engineering
IDS/IPS Configuration Audit
Firewall Configuration Audit
Endpoint OS Configuration Audit
External Penetration Tests
Laptop
IPS
Intranet
WS
WS
Laptop
Internal Penetration Tests
Internet
Router
Firewall
Router
Switch
Application Server Configuration Audit
Application server
FTP, App.
SQL
Print
File
Array
Router
Network Device Configuration Audit
Firewall Configuration Audit
Firewall
Switch
VPN, File
WS
Remote office
Switch
Router
HTTP proxy
SQL
SMTP
DMZ
Server OS Configuration Audit
Backup Configuration Audit
Server OS Configuration Audit
Endpoint OS Configuration Audit
Server OS Configuration Audit

centro

Wi-Fi wireless networks penetration testing

Complex screening of the wireless network architecture, of the level of security of each of its components and the related systems includes, besides other methods: attempts to penetrate and intercept, measuring the overlaps, detecting unauthorized APs, or the network permeability analysis.

Mobile devices penetration testing

Detailed analysis of architecture design for mobile communication, within the company and externally. Evaluating security levels of individual mobile devices or applications, in relation to the users using them, as well as to the other company assets.

VoIP penetration testing

Screening the voice communication systems operating over computer networks. Besides the testing common for the network devices, also the communication services specifics with impact to confidentiality, accessibility, and integrity of the transmitted information are being tested.

Supervisory control systems (SCADA) penetration testing Testing computer networks connected to components used to control and monitor industry technological equipment. This screening will uncover especially those weak spots within the architecture and security design of each component in the supervisory control system that could result not only in operating outages, but also in financial loss.

Each penetration test and audit is executed according to our own penetration testing methodology based on the generally valid standards, recommendations, and methodologies for security screenings execution (OWASP, OSSTMM, PTES, NIST, PCI-DSS, and others), which was created on basis the AEC specialists long-term experience.

Other services offered in addition to penetration testing

DoS (Denial of Service) testing

Testing the system resistance against attacks aimed at denial of the service provided by the system.

Hacking training

Training for the customer's administrators on methods and tools used by the hackers in order to understand better the way the attackers are thinking and how their attacks are executed. The aim is to apply this information to increase the level of systems they are administering.

Screenings based on defined methodologies

Testing and screening systems based on compliance with the defined methodology requirements, such as GDPR, PCI-DSS, SOX, and others.

References

- If you would like to know more about the way we work, please do not hesitate and ask about us in any of the following companies. These are only some of the recent and approved references.
- Zuno bank, AG – the bank selected us as a reliable partner for its market launch. We executed complete testing of all the bank's critical systems.
- ING bank N.V. – we performed extensive penetration tests of all the systems in the bank, and that not only for ING Czech Republic.
- We are regularly performing security testing for our customers such as AXA, T-Mobile, Komerční banka, KBC Group N.V., or Novartis.

centro

AEC

DATA SECURITY

AEC a.s.
Brno: Purkyňova 2845/101, CZ – 612 00 Brno, Phone: +420 530 507 200
Praha: European Business Center, Dukelských hrdinů 34, CZ – 170 00 Prague, Phone: +420 267 311 402
Bratislava: Prievozská 1978/6, SK-821 09 Bratislava, Phone: +421 254 410 283

www.aec.cz