Audits for systems and devices

AEC

Have you done some penetration tests but still aren't sure if the security of a particular server or other application platform is enough? Do you need to thoroughly test the security of key elements in your information system? The solution to these and many other problems is to make a detailed security audit of specific systems or devices within your organization's information system.

Whereas during penetration tests, AEC specialists take on the role of a potential attacker, during technical security audits they approach the element under investigation more in the role of a system administrator and implementer of measures recommended to improve its security. When checking the settings of individual systems, we use the knowledge and experience of AEC's security and system specialists, the manufacturers' recommendations for hardening systems and so on.

Every deficiency found is described in detail in the audit report. The risks of these vulnerabilities are described and, of course, suggestions for eliminating them (or risk minimisation) are also included.

www.aec.cz

Audits for systems and devices

During the technical audits we provide the following services

An audit of the configuration of active network elements

Active network elements are one of the riskiest places in the network and are often associated with a large number of unauthorised intrusions. Therefore, when analysing them, we mainly focus on the areas of static table settings on active network elements, network address translation (NAT) settings, network monitoring, administrative interface security, etc.

An audit of the configuration of operating systems on servers

The verification of the operating system (OS) configuration on servers is carried out using system resources and specialised tools. The security specialists scan each platform. Windows system auditing focuses on, for example, assessing password policy settings, audit policy, active directory, and so on. UNIX type operating systems are primarily checked from the standpoint of their configuration and the security of services (/etc/conf/) etc.

An audit of firewall and IDS/IPS configurations

The analysis is performed by firewall specialists who take up the position of an administrator to analyse the settings of these key security features. As concerns firewalls, they can audit both the application security itself and the defined rules. The primary result of the IDS/IPS analysis is an assessment of how suitable the client's system settings are and possible suggestions for optimising them.

An audit of the security of special systems, applications and services

Checking selected applications for their reliability, configuration, integrity, authentication and data confidentiality. This includes, for example, audits of application servers, database servers, web servers and many other applications and services, which may include areas such as the security of critical data flows, application errors, the possibility of application abuse, application stability, encryption implementation, PKI, etc.

Solution benefits

- Over 20 years of experience in the field of security in the Czech and Slovak Republics.
- A broad team of certified auditors and administrators with experience from scores of audits carried out every year.
- We use commercial, free and our own tools and scripts to collect data and subsequently analyse it.
- Evaluating the company's ICT security level and defining real risks in the context of the assumed impact on business.
- We conduct audits in accordance with the PCI-DSS and PA-DSS.

Other specialised audits

Audits in accordance with the PCI-DSS and PA-DSS

Specialised comprehensive audits that take into account the type of audited equipment and its location and connection to other IT infrastructure. It is not done as a single audit, but as an audit of the entire infrastructure.

Topology and infrastructure audits

An inspection of the network or cloud topology in operation from the standpoint of access security for third parties, partners, employees, proposed DMZ departments and the security of core systems, etc.

Methodology

When conducting security audits, we use an integral and continuously updated AEC methodology based on the methodologies and recommendations of some of the top organizations dealing with information technology security.

- Manufacturers' recommendations on the hardening of audited HW, OS and SW.
- Recommendations from the Internet Engineering Task Force (IETF) – an organisation releasing RFCs, called Internet standards.
- NIST recommendations (e.g. NIST SP 800-44 Guidelines on Securing Public Web Servers).
- CVE – Common Vulnerabilities and Exposures - a standardised dictionary of common vulnerabilities and threats.
- Common Criteria (ISO/IEC 15408) – a standard for assessing the security level of systems, etc.

Prague – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283