Penetration tests

Verify the security of your systems and applications before someone else does.

We carry out simulated cyber-attacks on systems, applications and entire infrastructures. Our range offers specific penetration tests for specific applications and systems. With Red Teaming exercises you can prove your ability to detect an attack and give the correct response by means of your processes and security specialists. We also offer a service that simulates phishing attacks using social engineering techniques.

Our aim is to detect threats and vulnerabilities that can compromise the confidentiality, integrity or availability of your systems and applications. Our work results in a final report that includes the vulnerabilities found with a description of how to replicate them, the severity of the potential risks, and recommendations for remediation. At the final workshop, we will familiarize your team with the progress of the tests and discuss the individual findings in detail, or, if needs be, the cooperation can be extended to include follow-up training on a given topic.

www.aec.cz

AEC

Services we offer

- **Penetration tests for applications**
  - Web
  - Mobile
  - Desktop
  - API
- **Penetration tests for infrastructure**
  - Internal
  - External
  - Stress tests / DoS
  - Wi-Fi networks
  - Control systems / ICS
  - VoIP
  - IoT
- **Configuration tests**
  - Operation systems
  - Cloud
- **Specialized tests and services**
  - ATM
  - RFID
  - Reverse Engineering
  - Phishing
  - Ransomware
  - Source code review
- **Tests via social engineering**
- **Red Teaming**

Penetration tests for applications

Web
Our aim when testing applications is to detect vulnerabilities that may compromise their confidentiality, integrity or availability. In the context of application security, we not only deal with common attacks exploiting typical vulnerabilities, but we also look at the application's design or architecture.

Mobile
During the mobile app tests, we look for bugs in their implementation and in the devices themselves. We analyse the apps' potential risks and look for safe solutions for using mobile devices in the corporate environment. We carry out forensic analysis on mobile phones that have been the target of hacker attacks and then use this experience to help create secure applications.

Desktop
For desktop applications, we use decompilation all the way to the source code level, including modifications. We identify security risk spots, sensitive data or other flaws in the authorization or the actual transmissions between the client application and the server.

API
Using API penetration tests, we test the weaknesses in the interface for providing services. For APIs, we test different types of interfaces, the most common being REST and SOAP. Whilst testing we use the relevant parts of the OWASP methodology for testing web applications as well as our own methodology that arose from our experience testing API services, PSD2 and others.

Configuration tests

Operation systems
For operating systems, we verify the individual configuration elements' level of security. We also offer to implement the recommendations that we make based on our tests' results, thus removing the weaknesses found and increasing your defences in the event of a sudden real attack.

Cloud
The migration of corporate infrastructure to the cloud is becoming a trend. The configuration of cloud services, be they native or third-party, plays a key role. Configuration shortcomings can lead to losing both company data and customer trust. This is why we are ready to help you with the issue of securely configuring your cloud environment.

Tests through social engineering

Social engineering is an act in which a social engineer attempts to get their target to do something that may not be in the target's best interest. Employees are considered the weakest security link in a company. Thus, an attacker can use social engineering to breach even the most secure perimeters. To do this, social engineers use attacks such as vishing, phishing, or physical infiltration through impersonation. Our aim is to examine your company's security using these methods and then propose the best solution to eliminate the risks found.

Penetration tests and infrastructure

Internal
During penetration tests on internal infrastructure, we map the company's internal network, identify active network elements and verify their security. We attempt to break into selected systems and compromise the company's domain by escalating privileges from an ordinary user to a domain administrator. Part of this also includes tests from a normal user's workstation.

External
During penetration tests on external infrastructure, we place an emphasis on discovering all the available network services, components and enumerating them in detail. Collecting public information about a company's network infrastructure is crucial for a hacker. We use both automated and our own proprietary tools and methodologies to do this.

Stress
If a company has key web applications, then attackers often damage companies' websites by simply making them inaccessible. The longer a web application is unavailable to users, the greater the losses. In the framework of Denial of Service, we test selected services to ensure that such situations do not occur and that critical web applications continue to function even under unexpectedly high load.

IoT
Our main aim when testing the Internet of Things (IoT) is to determine how easy a target the given devices are, what information can be extracted from them, and how to detect their vulnerabilities, ones that can be exploited to gain unauthorized access or steal data.

Wi-Fi networks
We use penetration tests on Wi-Fi technologies to simulate an attack on access to an organization's internal network by means of a Wi-Fi signal. After gaining access, we examine the quality of the traffic filtering between the network segment of the Wi-Fi clients and the rest of the internal networks. During our tests we also analyse the configuration for the connection to the wireless network on the part of the client devices.

SCADA
We will ensure that your control systems (SCADA) are secured against external and internal threats with the help of penetration testing. SCADA systems are often outdated and full of vulnerabilities, making them easy targets for APT attacks. Many systems have not been updated, for fear that they will malfunction or stop production, these flaws can then be easily exploited by attackers to take control of them.

VoIP
We provide penetration testing on an organization's publicly available critical infrastructure, such as VoIP phone systems. Using a "man-in-the-middle" method, attackers listen in on communications between incoming and outgoing phone connections. They can then gain access to sensitive data in the internal VoIP network. We will check all the weak spots to stop such situations from occurring in your organization.

Specialized tests and services

ATM

We scan for cashpoint vulnerabilities within a week. Our comprehensive analysis includes physical access methods, privilege escalation and tests on the operating system and applications. However, we can also focus solely on penetration testing for the infrastructure, integration services and management, reverse software analysis, or source code security analysis.

Reverse Engineering

During reverse engineering, we reanalyse the functionality of the applications under test, without access to or knowledge of their source code, thus verifying their resilience to potential real-world attacks. During the code analysis, we use our experience from penetration tests for desktop clients.

Phishing

We test companies' resistance to ransomware attacks. During this test we analyse existing situations, including system resilience testing. The output is a report with recommendations for the relevant solutions.

Codebashing

If you develop applications, we offer solutions for education and evangelism in application security by means of Codebashing. This enables security and development teams to create and maintain a culture of secure development. Through communication tools, gamification, peer challenges and ongoing assessments, Codebashing helps you eliminate software vulnerabilities from popping up in your source code.

Ransomware

We offer a unique service to test your organisation's resistance to ransomware. Can your security technology or mechanisms detect this type of malware? Are your employees sufficiently trained not to allow ransomware from running on your network? We'll tell you all about it.

RFID

With RFID technologies, we replicate publicly known attacks on specific types of cards and likewise we undertake our own investigation into possible vulnerabilities and potential attack vectors.

Red Teaming

With Red Teaming, we go far beyond the boundaries of classical penetration tests. We faithfully simulate attacks by real hacker groups and try to verify an organization is fully secure not only in the technological area, but also at the level of its internal processes and internal security specialists. In contrast to penetration tests, where a certain level of cooperation is normally required from the client, Red Teaming is a black box - we find out all the information about the target during the activity and try to remain hidden for as long as possible.

We have set up a community project in which we want to share know-how and build an attractive platform for regular meetings that move our members forward.
We deliberately skirt around the logic of tested products and systems. We hack their processes, looking for vulnerabilities, flaws in both implementation and security.

Come and join the programme to test IoT device security

We subject your device to analysis and write a detailed report describing the security vulnerabilities found with proposals for fixing them.

Give us a call if you are:

- IoT and smart technology manufacturers.
- Retailers who want to offer a high-quality service to their customers.
- Users who are unsure about the quality of their product's security.

Visit our website for more information about HackingLab, the community and collaboration opportunities.

hackingLab hackinglab.cz

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