# Cloud Security Assessment

## Cloudu Security

One of today‘s leading trends is the migration of corporate infrastructure to the cloud environment. On-premises security has been well-near perfected at many companies in recent years. However, the cloud environment brings new challenges and opportunities where existing tools and procedures are no longer effective. Responsibility can be transferred to cloud platform operators in many ways, in accordance with a shared responsibility model (SaaS, PaaS, IaaS, On-prem). The configuration of cloud services, both native and third-party services, plays a key role. Misconfiguration can lead to the loss of corporate data and customer trust, which is where we come in, ready to help you with the secure configuration of your cloud environment.

aec-security.eu

## Cloud Security Assessment

### Cloud perimeter security

An assessment of the security of cloud infrastructure exposed to the public internet in order to identify potential threats and risks that allow hackers to infiltrate or extract corporate data and other sensitive information from your cloud environment.

### Compliance tests according to security standards

Verification of the current configuration status of your cloud environment against best practices based on the CIS benchmark or sets of security metrics developed by cloud service providers and the security community.

### Configuration audit of selected services

Comprehensive verification of the current configuration of selected cloud services against a number of „best-practice“ and security recommendations using automated tools and enumeration frameworks, as well as a large number of manual tests and individual configuration verifications to identify deficiencies and offer optimal solutions.

# Cloud Security Assessment

AEC

To ensure the security of your cloud environment, we recommend regularly checking its configuration to ensure it complies with your business and other requirements. **Cloud Security Assessment** gives you the opportunity to remove unnecessary users, roles, groups and IAM policies, as well as ensuring your users and software only have the authorisation necessary to do their work.

## Cloud perimeter security

- Identification of IP ranges of cloud infrastructure.
- Enumeration of running services and their versions.
- Exploitation of detected vulnerabilities.
- Real simulation of a hacking or cyberattack (black-box testing).
- Identification of potential leaks of sensitive data and access.
- Detection of vulnerabilities due to service misconfiguration.

## Compliance tests according to security standards

- Determination of current configuration status.
- Verification against CIS/PCI-DSS/HIPAA.
- Evaluation of compliance or non-compliance with the selected benchmark.
- Proposal of a solution for established findings.

## Configuration audit of selected services

- You decide which cloud services will be tested in detail.
- We proceed based on a number of best-practice recommendations beyond the usual compliance tests. We draw on a variety of sources (Azure/AWS documentation, the security community, in-house experience, etc.) to offer you the best solutions.
- We offer a balanced manual and automated configuration audit by our specialists for selected native cloud services.

In general, our Cloud Security Assessment includes a security audit of your cloud solution in many areas, reveals various misconfigurations and provides you with a number of recommendations for maximum security, not just in the following areas:

- identity and access management,
- virtual privateí cloud,
- databases,
- network security groups,
- advanced threat protection,
- encryption, including secure key and password storage,
- application security,
- storage security,
- patches and instance management,
- tracking and monitoring configuration changes,
- and many other areas of the cloud.

## Our strengths

- We are one of the leading, reputable security companies in the Czech Republic and have been successfully doing business on the market for more than 30 years.
- We are constantly developing our skills and expertise in the field of security for cloud solutions.
- Our team consists of specialists with experience in projects on Azure and AWS cloud platforms.
- We are certified in many fields of web and infrastructure security. We also hold a number of cloud certifications and are hopig to achieve further security certification for both Azure and AWS.
- We run our own hacker laboratory for research in a number of areas dealing with the security of various solutions.
- We listen to clients and adapt tests to their needs and time constraints.
- We follow modern trends in cloud security.
- When testing, we continue to take a predominantly manual approach, which leads to the detection of design errors, as well as harder to detect misconfigurations of cloud services compared to automated tools.