Section 1

RESEARCH OF SECURITY OF INFRASTRUCTURE AS A CODE TECHNOLOGIES

Yudin O.V.
National Aerospace University «Kharkiv Aviation Institute»
Scientific adviser Tsuranov M.V.

Relevance. With the **growth** of companies providing cloud computing services, tools for definition Infrastructure as a Code (IaC) are gaining popularity rapidly. Modern business is trying to reduce the amount of time spent on deploying applications. After describing the desired project infrastructure, the developer is given the possibility to quickly deploy the environment without performing unnecessary operations with the New IaC approach.

According to statistics, 63% of IT companies partially use the approach of describing infrastructure with code, and 7% of all IT companies completely use this approach in their projects [1]. It is given significant advantages in convenience, speed, reliability, and standardization of the project.

However, not all specialists working with this technology check the security of the described architecture in practice. According to Snyk estimates, 38% of companies do not check the security of their infrastructure during the process of code delivery from the remote repository to the server that is responsible for the health CI/CD of applications, and also do not think about checking static vulnerability scanners [1].

The purpose of this work is to investigate the mechanisms of protection confidentiality of cloud infrastructure, in case of vulnerabilities that arise from an incorrect description of the infrastructure code.

There are a plurality number of threats aimed at revealing the confidential information of a project described using IaC, such as architecture data, passwords, keys, etc.

According to OWASP, the threat disclosure of confidential information occurs in 19.84% of projects [2]. In the OWASP list, the aforementioned threat is called differently but is directly related to it, namely A05:2021 - Security Misconfiguration. This is on account of the fact that in a test project it is much more convenient to immediately place the credentials in the code.

The problem is that the developer may not remember to delete sensitive data after performing certain tasks when changes need to be submitted to the version control system. Such inattention is observed by 24% of cloud infrastructure developers and can completely compromise the customer's company, because initially, before the targeted attack, the attacker will conduct an OSINT investigation of the victim [1].

Principal provisions. To timely validation the code for the presence of sensitive information, as well as validation for vulnerabilities inside the software libraries used, it is possible to use special static scanners that will detect vulnerabilities accidentally or intentionally embedded in the source code [3]. There are many vulnerability scanners in the community for different tasks. In most cases, the customer uses scanners such as Snyk, Clair, and Trivy.

It is also worth noting that many version control systems already have mechanisms for checking the code being loaded into the repository for the presence of authorization keys. However, such solutions can only detect and exclude those keys that are created directly by the version control system, which is not enough to ensure the security of the project infrastructure.

Conclusions. The Infrastructure as a Code technology helps flexibly configure and administrate the required project architecture. However, there are abundant threats, part of which are not obvious and need exploring. One of the non-obvious threats is exposing sensitive information from the variable by intercepting network traffic over an unsecured network. The thesis considers the main threats and vulnerabilities in describing IaC technology, which could be profitable and exploited to attack privacy.

List of references

1. Snyk research report, Infrastructure as Code Security Insights. – Snyk. – February 2021.
2. A05:2021 – Security Misconfiguration. OWASP Top 10:2021. URL – https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ (дата звернення: 21.06.2022).
3. Савчук В. О., Цуранов М. В. Аналіз засобів безпеки хмарних платформ. У кн.: Проблеми інформатизації: тези доп. 8-ї міжнар. наук.-техн. конф., 26-27 листопада 2020 р., м. Черкаси, м. Харків, м. Баку, м. Бельсько-Бяла : [у 3 т.]. Т. 1 / Черк. держ. технолог. ун-т [та ін.]. – Харків : Петров В. В., 2020. – 83 с.

Information about the authors

Yudin Oles Viktorovich, a master`s student from the Department of Computer Systems, Networks and Cybersecurity, phone number 066-554-94-07, o.yudin@student.csn.khai.edu

Tsuranov Mikhail Vitalievich, information security researcher and advisor