The NSA identifies 4 'critical' security vulnerabilities of cloud systems

The US National Security Agency (NSA) has issued a new guide to help organizations and businesses improve the security of data stored on the cloud.

According to CSO, more than 80% of organizations and businesses have been using services from 2 or more public cloud infrastructure providers, and nearly 2/3 of them It is using the service of 3 or more providers.

In the face of cloud computing becoming an integral part of every field, the US National Security Agency (NSA) has issued a new guide to help organizations and businesses improve Security of data stored on the cloud. Let's take a look at the four most notable security holes in the NSA recommendation below.

According to NSA experts, vulnerabilities in cloud systems can be divided into four categories: misconfiguration, poor access control, common shared and supply chain vulnerabilities.

Wrong configuration

This is the most common cloud vulnerability. Cloud-based resources are complex and constantly changing, making it difficult for system administrators to configure.

Wrong configuration may allow an attacker to access data and cloud services. In May 2017, this type of security flaw caused a huge amount of confidential data of one of the largest defense corporations in the United States to fall into the hands of hackers, causing millions of dollars in damage. Similarly, in September 2017, a security researcher discovered CENTCOM data that could be publicly accessible to all public cloud users. There are countless examples of cloud security disasters associated with misconfiguration.

Poor access control

This happens when cloud services use weak authentication methods or contain vulnerabilities that make it easier for hackers to bypass authentication layers. Weaknesses in access control mechanisms can allow an attacker to gain system privileges, thereby compromising cloud resources.

Continuous cyber attacks in October 2019 from the Phosporous hacker group targeted Microsoft customers, and the March 2018 attack of the Iranian Mabna group that caused email accounts to be compromised by omitting multi-factor authentication, are examples of how this vulnerability could be exploited by threat agents.

Shared vulnerability

Cloud platforms often consist of many software components and hardware combined. Highly skilled hackers are able to identify hardware and software components used in the cloud architecture and take advantage of the vulnerabilities inside these components to gradually penetrate the system.

This type of attack is very rare, but once it takes place, it is difficult for businesses to detect, and damage is almost inevitable.

Supply chain gaps

Supply chain vulnerabilities in the cloud include the presence of internal threats and intentional backdoors in hardware as well as software. In addition, third-party cloud software may also contain intentionally or unintentionally created vulnerabilities, thus becoming a threat to the entire system. Cloud service providers must be able to control and remedy all holes in the supply chain.

Managing risks in the cloud is the responsibility of cloud service providers (CSP). Therefore, CSP should implement appropriate countermeasures to help customers secure cloud resources. Cloud security is an ongoing process and customers should also actively monitor their cloud resources. Please report immediately to CSP if any abnormalities occur.