GUIDANCE

Cloud security guidance

Guidance on how to configure, deploy and use cloud services securely

IN THIS GUIDANCE

PUBLISHED

17 November 2018

REVIEWED

17 November 2018

VERSION

1.0

Implementing the Cloud Security Principles

Details and context for the 14 Cloud Security Principles, including their goals and technical implementation

For each of the 14 principles, we answer three questions:

Back to top

1. What is the principle? A description giving the principle some context
2. What are the goals of the principle? Concrete objectives for the implementation to achieve
3. How is the principle implemented? Details for a set of possible implementations

1. Data in transit protection

User data transiting networks should be adequately protected against tampering and eavesdropping.

2. Asset protection and resilience

User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.

3. Separation between users

A malicious or compromised user of the service should not be able to affect the service or data of another.

4. Governance framework

The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.

5. Operational security

The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.

6. Personnel security

Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.

7. Secure development

Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.

8. Supply chain security

Back to top

The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.

9. Secure user management

Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.

10. Identity and authentication

All access to service interfaces should be constrained to authenticated and authorised individuals.

11. External interface protection

All external or less trusted interfaces of the service should be identified and appropriately defended.

12. Secure service administration

Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.

13. Audit information for users

You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.

14. Secure use of the service

The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.

← 13: Audit informatio...

1. Data in transit... →

Topics

Cloud

PUBLISHED

Back to top

REVIEWED

17 November 2018

VERSION

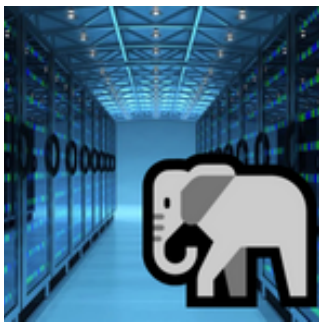
1.0

Also see

Defending software build pipelines from malicious attack

Compromise of your software build pipeline can have wide-...

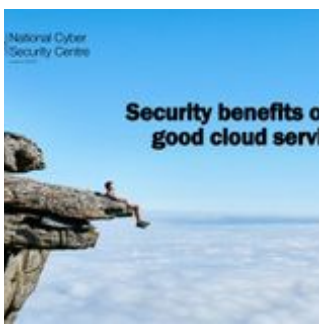
Blog Post
3 February 2021



The elephant in the data centre

A new white paper from the NCSC explains the potential benefits of...

Blog Post
13 November 2020



Security benefits of a good cloud service

How to plan and configure your cloud service to maximise securit...

Whitepaper

Back to top