BLOG POST

Personnel security in the cloud

Making sure you minimise your cloud provider's access to your data.

Jamie H

Whenever you use a third-party supplier, you need to consider their approach to personnel security. Cloud suppliers are no exception.

Since the NCSC Cloud Security Principles were first released back in 2014, we've covered this topic in Principle 6: Personnel security. Traditionally, this has focused on security screening (often called vetting) and ensuring that as few people as possible have access to your data.

However, the cloud has evolved since 2014, so we've recently updated our guidance to reflect how personnel security has changed. This blog summarises what's changed, and why it matters.

Making access granular

While security screening and limiting who has access to your data are both important aspects of personnel security, they will only get you so far. In a hyperscale cloud provider, this could still be several thousand people, working around the globe. Security screening and limiting alone still leaves a significant risk of malicious or accidental access to data. Instead, you should expect your cloud provider to take a more layered approach.

A good cloud provider will also apply technical controls to bring additional defence in depth. A well-designed cloud service will allow a support engineer to diagnose and treat the fault without having to access customer data in a large number of cases. For example, all access to customer data and services should be audited

cases. For example, all access to customer data and services should be audited and monitored in detail, to discourage inappropriate access and help investigate incidents. You should also be alerted whenever your cloud provider's personnel access your data, so you can confirm that this was expected.

When you store sensitive data or operate an important service on a cloud service, you should expect even more advanced protections. For example, to access your data, your cloud provider's personnel should have to supply a customer support ticket (or internal change request) to justify the access. Ideally, you should also have to authorise each access to your data, and be provided enough context to allow you to make an informed decision.

Secure system administration

When we discuss personnel security, it's also important to cover Principle 12: Secure service administration. This is closely aligned with our wider Secure system administration guidance. While Principle 6 focuses on an insider maliciously or accidentally gaining inappropriate access to data, Principle 12 ensures an outside attacker can't interfere with your use of the cloud by compromising the service's administration. Remember that some of this administration will be performed by support personnel, who may not fit the traditional model of 'system administrators'.

The two principles work hand in hand, each supporting the other. A cloud provider that applies excellent technical controls will also make it much harder for an outside attacker to access customer data. At the same time, secure system administration will prevent an insider from circumventing the technical controls that keep them honest.

The silver lining

A good cloud provider will design their service so that you don't need to explicitly trust all of their personnel, allowing you to focus on building trust in the service as a whole. Our updates to the 14 Cloud Security Principles have raised the bar considerably for personnel security, and we're already seeing organisations doing this well. This should serve as a reminder that using a good cloud service will often bring security benefits that would be hard to achieve in traditional deployments.

Jamie H
Senior Security Researcher

WRITTEN BY

Jamie H
Senior Security Researcher

PUBLISHED

17 November 2022

WRITTEN FOR

Cyber security professionals

Large organisations

Small & medium sized organisations