FUJITSU

Cloud Security Speak
Glossary

Cloud Security Speak

Cloud computing is demonstrating its potential to transform the way IT-based services are delivered to organisations. It can and will create substantial business benefits through reduced capital expenditure and increased business agility.

For most organisations, therefore, the journey to cloud is no longer a question of "if" but rather "when", and a large number of enterprises have already travelled some way down this path.

There is one overwhelming question that is still causing many organisations to delay their move to cloud: Is cloud computing secure?

Here is a quick guide to key terminology used in Cloud Security for those involved in investigating and evaluating solutions for their organisations.

Access control

A way to control who and/or what may access a given resource, either physical (e.g. a server) or logical (e.g. a record in a database).

Architectural patterns

A design model that documents how a solution to a design problem can be achieved and repeated.

Availability

The proportion of time a system is in a functioning condition, based on a number of performance measures such as uptime.

Big data

Data sets that grow so large that they become awkward to work with using traditional database management tools. Typically contains many small records that are travelling fast.

FUJITSU

shaping tomorrow with you

Cloud Security Speak

Business continuity (BC)

(See also: Disaster recovery) Business continuity involves planning to keep all aspects of a business functioning amid disruptive events (whereas disaster recovery focuses on restoring or replicating the IT systems and services that support business functions).

Certification

Documentary confirmation that a service, product, person or organisation conforms to certain characteristics or possesses particular skills. This is often, but not always, subject to some form of external assessment.

Cloud architecture

The architecture of the systems involved in the delivery of cloud computing. This typically involves multiple cloud components communicating with one another over a loosely-coupled mechanism (i.e. one where each component has little or no knowledge of the others).

Cloud server buyer (CSB)

The organisation purchasing cloud services for consumption either by its customers or its own IT users. (Also referred to in this book as "the buyer".)

Cloud service provider (CSP)

A service provider that makes a cloud-computing environment – such as a public cloud – available to others.

Cloud services stack

The different levels at which cloud services are provided. Commonly; Infrastructure-as-a-Service (Iaas), Platform-as-a-Service (PaaS); Software-as-a-Service (SaaS); Data-as-a-Service; and Business Process-as-a-Service (BPaaS).

Confidentiality

The act of keeping data secret within a certain circle, where that information is not intended to be known publicly.

FUJITSU

shaping tomorrow with you

Cloud Security Speak

Context-sensitive

(When referring to a system) Exhibiting different behaviour depending upon the task or situation (for example, presenting data differently on different classes of device, such as personal computers, tablets and smartphones).

Data residency

The location of data in terms of both the legal location (the country in which the cloud service contract is enforced) and the physical location (i.e. the data centres where it is stored).

Disaster recovery (DR)

(See also: Business continuity) The process, policies and procedures related to recovery or replication of technology infrastructure after a natural or human-induced disaster. DR is a subset of business continuity.

Distributed denial-of-service (DDoS) attack

An attempt to make a computing resource unavailable to its intended users by bombarding it with many simultaneous connection requests. "Distributed" refers to the use of multiple, dispersed systems to attack the resource.

Federation

The provision of security to allow for clean separation between the service being accessed and the associated authentication and authorisation procedures. This enables secure collaboration across multiple systems, networks and organisations employing different security systems.

Hash

A means of checking data integrity using a short code mathematically generated from the original data. Any accidental or intentional change to the data will change the hash value.

Hypertext Transfer Protocol Secure (HTTPS)

A secure protocol for the transfer of encrypted communications across a computer network.

FUJITSU

shaping tomorrow with you

Cloud Security Speak

Hypertext Transfer Protocol Secure (HTTP) with SSL/TLS

Protocol to provide encrypted communication and secure identification of a network web server.

Integrity

In the context of data security, integrity means that the data cannot be modified without detection.

Interoperability

The ability of diverse systems and organisations to work together.

Linked data

A concept (famously championed by the web's inventor Tim Berners-Lee) in which structured data is published in a standard format so it can be interlinked and queried or read by both humans and machines. This facilitates the widespread use of multiple, diverse data sources in the creation of services and applications.

Non-repudiation

A service that provides proof of the integrity and origin of data together with authentication that can be asserted (with a high level of assurance) to be genuine.

Outsourced service provider/managed service provider (OSP/MSP)

An external provider who manages and assumes responsibility for delivering a defined set of services, either proactively or as they are needed.

Patriot Act

The USA Patriot Act, a law enacted in the US, formerly known as the Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act of 2001.

FUJITSU

shaping tomorrow with you

Cloud Security Speak

Personally identifiable information (PII)

Data that, by its nature, is covered under privacy and data-protection legislation. This applies to information about both employees and consumers.

Real time

Real-time programs must guarantee a response (from event to system response) within strict time constraints. A real-time system may be one where the application is considered (in context) to be mission-critical.

Service level agreement (SLA)

Part of a service contract where the level of service is formally defined to provide a common understanding of services, priorities, responsibilities and guarantees.

Shadow IT

A term often used to describe IT systems and IT solutions built and/or used inside organisations without formal approval from the IT department.

Security information and event management (SIEM)

A solution to provide real-time analysis of security alerts generated by network hardware and applications; also used to log security data and generate reports for compliance purposes.

Single sign-on (SSO)

A mechanism whereby a single action of user authentication and authorisation permits access to multiple systems without the need to enter multiple passwords

Security operations centre (SOC)

A business unit that deals with security issues on both an organisational and a technical level.

FUJITSU

shaping tomorrow with you

Cloud Security Speak

Tokenisation

The process of replacing a piece of sensitive data with a value that is not considered sensitive in the context of the environment in which it resides (for example, replacing an item of data with a reference to the actual data which is held in another database and hosted in a different environment).

Uptime

(See also: Availability) A measure of the time that a computer system has been available for service. Not to be confused with overall system availability, which will depend on a number of measures, including the uptime of individual components.

Vulnerability management

The cyclical practice of identifying, classifying, remediating and mitigating vulnerabilities.

If you approach cloud in the right way, with the correct checks and balances to ensure all necessary security and risk management measures are covered, you can manage your exposure to risk appropriately.

We can help you to make informed security decisions about your cloud set-up and better understand how to securely reap the benefits of cloud.

Discover more at **uk.fujitsu.com/secure-thinking** where you can find these useful references:

- The white book of Cloud Security
- Cloud security checklist
- Is cloud computing secure? (Infographic)
- What's the real issue with Cloud Security? (video)

Contact us on:
Tel: +44 (0) 870 242 7998
Email: askfujitsu@uk.fujitsu.com
Web: uk.fujitsu.com