BIZCOMMUNITY

An end-to-end approach is critical to securing cloud computing

By Roelof Louw

22 Feb 2013

Cloud computing is predicted to be the future of the technology world and analyst reports abound on the expected growth of the uptake of these solutions. However, security issues remain one of the dominant barriers with the adoption of cloud solutions.

Many organisations are hesitant to migrate to the cloud in light of the ever-increasing number of attacks on cloud-based solutions, as well as the risk of downtime cause by natural disasters and other issues in the regions where cloud data is stored.

When making the transition to the cloud, it is critical to adopt an end-to-end approach that focuses on IT security, data protection and availability, enabling organisations to leverage the multiple benefits of the cloud while minimising the risks. Furthermore, it is crucial to factor in both the internal and external risks associated with cloud computing, which, too, require a holistic approach.

This, in turn, requires that all potential threats be identified and structured protection mechanisms are put into place that go beyond technology and incorporate processes and people across multiple areas. There are 12 elements that should be considered to ensure the security of both data and applications when moving to a cloud platform.

1. Identity management

Identity management, including roles and rights, end-point security and access control, is a cornerstone of any ICT security solution, but is particularly important when it comes to the cloud. If employees can access business-critical information, there is always a risk that this will be misused, and if outside persons can access this information the danger is even greater. Thus, applying stringent identity management, security and access control on a need-to-know basis is a vital foundation component of an end-to end cloud security solution.

2. Secure communication into the cloud

With cloud services it is essential that data not be compromised when transferring between the user and the service provider. When data is sent over public networks such as the Internet, it must be encrypted to prevent access by unauthorised parties, to safeguard integrity and confidentiality. Secure remote access should be enabled using a Virtual Private Network (VPN). Security can also be enhanced using a Multi-Packet Label Switching (MPLS) VPN, which ensures that data streams sent by different users and services are strictly segregated. Before migrating to the cloud, organisations need to appraise their requirements to identify business-critical applications, to ensure that necessary bandwidth, Quality of Service (QoS) and prioritisation are delivered to ensure seamless service.

3. Transparent contracting within the cloud

Cloud applications can be distributed across multiple data centres, and the availability, confidentiality and integrity of data exchanged by cloud services and distributed applications within the cloud must be protected at all times. Data can also be moved from one data centre to another in order to create back-ups or improve resource utilisation. More complex cloud offerings often integrate third-party services, which makes visibility and transparency into the value chain critical. It is essential to specify clearly in contracts which services will be delivered by whom, and who is legally responsible in the event of any issues.

4. IT systems in data centres

When deploying cloud solutions, additional security measures are required at the data centre. Cloud computing is based on multiple clients sharing the same hardware and software; therefore it is important to implement mechanisms to safeguard systems, applications and data. This requires virtual segregation of users to ensure that they cannot access another user's data and compromise the integrity of systems. Data should also be isolated in dedicated network storage areas, similar to hard drives, which are accessed by the user's servers via the network. These should be connected in such a way as to ensure that customers can only access their own data, as though they had their own dedicated drive.

5. Protecting IT systems on the service provider side

To ensure the right level of security, mechanisms that protect systems, platforms and applications must be implemented at the data centre. In addition, there needs to be a secure link between the IT components stored at the data centre and the connection to the outside world. To ensure effective protection of the network segments, service providers need to employ two different types of firewall. Firstly, they require firewalls that perform stateful inspections of communications, ports and applications. Secondly, they need deep-inspection firewalls that can scan data-transfer protocols for "good" and "malicious" queries. Further key mechanisms include proxy servers and reverse proxies that filter and convert both incoming and outgoing data traffic, shield sensitive information, minimise vulnerabilities and help make ICT more secure.

6. Data centre security

Buildings and hardware assets at the data centre require physical security as well as technology security, including physical access control and intrusion detection. Data centres must be constructed to enable the building to withstand natural hazards, such as storms and hailstones, potential physical sabotage and fire. The facility must be located away from regions that are susceptible to heavy storms, flooding and earthquakes, and must meet a host of other criteria to ensure smooth operations and customer data security. Data centre protection should also include alarms, fire detection, surveillance, vehicle monitoring and control, and extensive staff checks to prevent attacks from within.

7. Security management and secure administration

The human factor not only plays a pivotal role in the security of cloud services for users. It is also an extremely important issue for the service providers themselves. For this reason, providers should operate a dedicated information security management system (ISMS) which defines processes and rules for the effective management of information security. Cloud providers must also draw up rules that ensure employees meet security requirements and specify which users can access which systems and data and who is responsible for which operational and security-related tasks.

8. Service management and availability

Application downtime can be detrimental for business, particularly when mission-critical systems are affected. As a result, organisations using the cloud must be involved in the definition of appropriate service levels. Service providers need to safeguard availability by creating redundant systems and back-ups that allow system recovery following downtime.

9. Contracts, process integration and migration

The scope and type of ICT services must be defined in a written agreement.

Requirements must be outlined and any necessary changes need to be implemented and monitored. Organisational structures and processes must be in place to enable a rapid response to security incidents or threats. Services must be clearly defined in a service level agreement (SLA), and mission-critical applications need to be identified to ensure the correct levels of availability and security. Documents should also outline emergency procedures, including the sequence in which systems will be reactivated following failure or downtime.

10. Security and vulnerability management

To avoid migration issues, any weaknesses or faults in infrastructure must be identified and addressed from the outset. This involves comprehensive testing and risk assessment. Security is a central issue across the entire lifecycle of an ICT system. This begins with documentation and correct management of configuration data. In addition, installation and configuration processes are key concerns. The proactive management of vulnerabilities and other developments designed to offer visibility into and enhance security and eliminate breaches in advance are also critical.

11. Security reporting and incident management

Visibility into the degree of security achieved is critical for mitigation of business and legal risks with regard to the impact on IT-supported business operations and potential compliance breaches. Security reporting provides this visibility, offering insights into the effectiveness of the protection mechanisms in place. Analysing this data enables measures to be modified, replaced or enhanced as required, leveraging the information available for proactive corporate risk management.

12. Requirements management and compliance

Users must comply with legal, regulatory and industry-specific requirements, including in-house policies, contracts with customers, suppliers and partners, and other obligations. Users need to verify that their cloud service provider can meet these imperatives. Data-protection legislation varies widely from country to country. Organisations also differ in terms of processes and potential threats, and the extent to which security incidents would negatively impact the business. A strong cloud service provider partner should offer a secure and assured route to the cloud, aligning it with the company's specific business context and requirements.

In light of the ever-growing threats, IT security is becoming increasingly complex, costly and time consuming, and increasingly complex technical requirements and rising costs of ensuring effective security are set to make outsourcing and cloud computing ever-more-popular alternatives to in-house operation. However, organisations need to select cloud service providers carefully, in order to ensure services are delivered in a secure, compliant manner and that risks both internal and external can be minimised.

Download the T-Systems Cloud Security white paper.

ABOUT ROELOF LOUW

Roelof Louw is cloud expert at T-Systems in South Africa.
- Going cloud - addressing the data centre dilemma - 19 Apr 2013
- An end-to-end approach is critical to securing cloud computing - 22 Feb 2013
- Follow the private cloud for secure business operations - 1 Oct 2012

View my profile and articles...