TREND MICRO

A Brave

Who Owns Security in the Cloud?

A Trend Micro
Opinion Piece

February 2011

Written by Dave Asprey,
VP Cloud Security

WHO OWNS SECURITY IN THE CLOUD?

I. WHO OWNS SECURITY IN THE CLOUD?

Cloud computing is the technology buzzword of the moment. The provision of on-demand IT software and infrastructure services via the internet can provide IT teams with unparalleled benefits in efficiencies, cost savings and scalability. However, with these game-changing benefits come a whole new set of challenges which invalidate most traditional approaches to security. The paradox at the heart of this new computing paradigm is that while the cloud in one sense offers a vision of simplified, pay-per-use IT in which much of the heavy lifting is outsourced, it also introduces numerous new compliance headaches and potential areas of data security risk.

Whether by their own initiative or having been forced by the business, IT managers are reassessing their options in this 21st century computing environment. They want to know the risks involved and crucially where the security responsibility and accountability lies.

Here we attempt to address these issues in the context of the Infrastructure as a Service (IaaS) – that which allows IT managers to rent networking, storage, server and other operational elements. It also offers enterprises greater autonomy to put more security controls in place than models such as SaaS.

II. WHY THE CLOUD?

On the public cloud side it all comes down to scaling and the ability to use opex (Operating Expense) instead of capex (Capital Expense). Cloud computing customers avoid capital expenditure on hardware, software and other infrastructure services by paying their provider only what they use, in a utility model. The on-demand provision of resources also allows firms to scale dynamically according to their computing needs in real-time, vastly improving business agility.

On the private cloud front, it is all about increased flexibility and responsiveness to internal customers' needs.

With these kinds of benefits it's unsurprising to see such interest in the new computing paradigm. Cisco research from December, for example, revealed that 52 per cent of IT professionals globally already use or plan to use cloud computing in the next three years. A similar poll from security body the ISACA (March 2010) found that a third of European organisations are already using cloud computing systems, while global consultancy Accenture revealed (July 2010) that half of its clients are running some mission critical apps in the cloud.

III. PERIMETER SECURITY ISN'T DEAD — TWO APPROACHES TO SECURING THE CLOUD

Much has been made of the fact that when it comes to the public cloud model, the traditional enterprise security perimeter simply doesn't exist anymore. Firewalls, intrusion prevention systems and other standard security functionality, the argument goes, can't extend to the cloud and instead firms have to rely on the very basic level of perimeter protection offered by their cloud provider.

But from another perspective the perimeter-based security model isn't actually dead at all, it's become a useful part of a working security architecture, but not the only part. When dealing with the cloud, enterprises still have the notion of a perimeter. The choice for firms is whether they extend that perimeter into the cloud or extend the cloud inside their perimeter, or both. In either case, additional security layers are necessary, just as they are in internal enterprise security environments. However, both scenarios have similar drawbacks concerning the potential lack of visibility and control arising from outsourcing to the cloud. CISOs must be vigilant, conduct due diligence and be aware of the risks involved.

1) The first scenario, extending your perimeter to the cloud, involves setting up an IPSec VPN tunnel to your public cloud provider's servers, and putting enterprise-grade security on the public cloud server, usually in the form of security software and virtual appliances.

The **benefit** of this set-up is that you won't have to reconfigure Active Directory and most other existing management tools should work with your cloud set-up, as your cloud severs are effectively inside your "perimeter".

However, on the **cons** side, depending on how well you secured your cloud server, you may have introduced the risks associated with the cloud to your architecture [outlined below]. To help mitigate these it's important that the link between cloud and internal servers be monitored for suspicious traffic, just as all links to critical servers should be, whether they're in a cloud or not. Another option is to add an extra DMZ and firewall, although that creates another perimeter to secure.

Many firms forget or ignore this step in their rush to the cloud, especially those in smaller organisations without the time and IT resources to architect in these safety barriers.

It's also essential to put enough security on those cloud servers so you can trust them – IDS/IPS bi-directional firewall etc.

RISKS

CIOs must be aware that their cloud servers will be subject to different threats from the ones they are used to mitigating internally.

- A major concern is that firms are not likely to be given their cloud provider's physical or admin access logs. How will they know if an IT admin working for their public cloud provider has accessed their data, for example? The insider threat can be mitigated to an extent internally by maintaining access logs, but this lack of visibility in the cloud should force the widespread adoption of data encryption as standard.

  [*In December it emerged that corporate data belonging to customers of Microsoft's hosted business suite BPOS was accessed and downloaded by other users of the software after a misconfiguration error. Although fixed quickly, it highlights what can potentially go wrong, and the importance of having visibility into your cloud provider's systems to ensure they meet your own and your regulators' standards*.]

- Shared storage also presents an area of risk to firms anxious that their data is not safe if sat alongside a competitor's data on the same disk in the cloud.

- Some public cloud providers simply aren't as hot on security, or as transparent about what they are doing, as they should be. As a starting point, if you're putting mission critical data into the cloud you at least need to look for strict adherence to security best practices, like ISO 27001 and SAS70 II, and rigorously examine your provider's SLAs and security policy.

- Related to the previous point is the fact that most cloud providers are likely only to reimburse in the case of a breach up to the cost of the service they provide, even if it was their fault. A data breach which leads to untold reputational damage, fines and financial loss potentially running into the millions, for example, will have to be absorbed by the customer.

2) The second scenario, extending the cloud into the enterprise, allows the cloud to effectively extend inside your perimeter, and involves agreeing to an IaaS public cloud provider or cloud-based MSSP installing a cloud node on site.

The **benefit** of this set-up, which is starting to become increasingly common among larger enterprises, is that it is a relatively well understood model. Akamai, for example, has done a similar thing for over ten years now, managing a server located within the customer's security perimeter, and MSSPs such as Integralis have been providing remote firewall management services "from the cloud" for years. Other examples include the Trend Micro Smart Protection Network, which links security servers inside an enterprise network to a security network of thousands of servers in the cloud.

However, for all the simplicity of having one of these boxes located in your data centre or branch office and managed or updated centrally by the cloud provider, the main **cons** are that it is still essentially a cloud service and as such could present the IT manager with many of the risks of the first set-up.

- The risks presented by lack of visibility into physical and/or admin access logs remain

- Liability for negligence leading to loss of your mission critical data will still only go as far as reimbursement for the cost of the service.

- Although it can be turned on and off, when it's on the cloud provider will have access to your network and application data so it must be trusted. If that provider is focused on security and transparent with its SLAs, there should be less to worry about. However, as discussed, most generalist cloud providers do not have security at the heart of their value proposition.

  It's about differentiating between 'good enough' security and 'optimal' security. A cloud-based email service set up in your perimeter by a managed security service provider, for example, is likely to be more trustworthy than one provided by a typical public cloud vendor.

IV. SO WHO OWNS SECURITY IN THE CLOUD AND WHERE ARE THE GAPS?

The unpalatable truth here is that if you're looking for help from the cloud provider you're likely to be disappointed, in fact, you may even find your job made more difficult by the lack of visibility you have into access logs or the disconcertingly vague wording of security policies.

- You should secure your cloud servers as you secure your internal servers. This includes; IDS/IPS, DLP tools, bi-directional firewall, and encryption.

- You could run into problems on the network security front in the cloud environment, as few public cloud providers are likely to allow you to monitor network traffic as closely as you'd like. In your own network, all router/switch configuration and logs are free, and you can sniff any network traffic you want. But in the cloud, none of that is available. This may rule out the cloud from a compliance point of view, so it's vital you find out how much network monitoring and access your provider will allow.

- Encryption of data at rest and in transit becomes extremely important because of the lack of visibility into network traffic and your provider's admin access logs.

- Many cloud providers also offer a worrying lack of role-based access controls at an admin level. With Amazon EC2, for example, one account owns all the boxes, so one member of the organisation with account access could effectively have the keys to the kingdom, with the ability to add and subtract boxes at will.

- In the private cloud, ownership of security by the IT department is being challenged thanks to the speed at which servers can be created. That natural equilibrium between IT's ability to deliver the servers and the business' need for them is becoming unbalanced as the process accelerates. All the business needs today is to know it can cover the cost of a licence, and in a private cloud environment a business unit could have a server up and running in 1-2 days, rather than 6 weeks.

  However, each request for a new server has to be properly managed because the security risks will increase as the number of boxes to manage increases. It's important IT managers put in

place a central authorising process which ensures that any requests from the businesses must pass through IT first.

V. CALL TO ACTION

Enterprises

Encrypt data at rest and in motion and be careful to store encryption keys in a location separate from the data, i.e. not where they are easily accessible to the cloud provider.

Deploy every security tool you deploy on your physical servers in the cloud as well because all the cloud providers will give you is a naked OS without adequate security.

Cloud providers

Be more open and transparent about security policies and procedures around access controls and network traffic. Customers need to know who did what and when, and they need to be allowed to see the logs.

Clarify SLAs so customers are clear what security features you offer and what they will need to do to ensure their data is secured to their own and their regulators' standards.

Private cloud environments

Create a central authorisation process if there is not one already for all new cloud server requests from the business. You need to know why they need one, what will be running on the server, how long it will exist, how much traffic will flow through it and have regular check-ups on these requirements.

Be prepared....IT is being forced to accelerate the speed at which it works. For the good of the business you must be prepared to support these requirements in a timely manner without compromising on security.