


In for stormy weather

Highly publicised incidents involving cloud services threaten to undermine one of IT's hardest-hyped innovations. But is there a sure-fire way of securing the cloud?



Cloud computing has undoubtedly been one of the most hyped developments in enterprise IT over the last few years. This assessment is not without qualification though, as the benefits the cloud pledges include reduced capital spending costs, greater organisational agility, and simpler management of applications and IT infrastructure.

However, the question of cloud computing's security, or perceived lack of, has become a major point of contention. Cloud critics and cloud sceptics will therefore have felt somewhat vindicated in recent weeks as two highly-publicised incidents concerning popular cloud services to some degree ratified their fears.

The first of these involved US e-commerce giant Amazon's Elastic Compute Cloud (EC2), arguably the best-known of all enterprise cloud services. In the early hours of April 21, the infrastructure-as-a-service (IaaS) platform began experiencing technical problems, impacting the accessibility of popular social networking sites hosted on the service, such as Foursquare and Quora.

The glitch, which Amazon claimed was triggered by a "networking event" at its Virginia data centre, continued to detrimentally affect users of EC2 several days after the problems began. A small amount of volumes stored on the service were said to be lost for good.

Before the dust had even settled on the Amazon incident, another cloud catastrophe hit the headlines, when electronics behemoth Sony reported that security of its online video game platform PlayStation Network had been breached by hackers. In the fallout of this event, Tokyo-based Sony admitted that up to 100 million players' personal data had been stolen, a not insignificant volume of this related to users' credit cards.

Despite these incidents, and several other prominent examples in the recent past, cloud computing is gaining traction among enterprises. A report published by IT analyst firm Ovum in May 2011 showed that 45% of multinational businesses around the

world had adopted cloud services to some extent, compared to 28% when a similar investigation was conducted last year.

Further research shows that rising cloud deployments have not coincided with more stringent security measures. A separate investigation, by the Ponemon Institute in association with CA Technologies, found that 79% of surveyed cloud providers allocated less than 10% of their resources towards security. Perhaps more tellingly, 69% of these vendors claimed that security was entirely the responsibility of the end user.

It is no wonder then that IT industry security experts continue to warn and advise businesses on how to ensure a safe passage to the cloud.

CLOUDED HOUSE

James Lyne, senior technologist at Oxford, UK-based IT security firm Sophos, believes that at least some of the complexities around cloud security stem from the muddy definitions of the concept itself. "One of the biggest challenges with cloud is that it's a vague term that gathers together a huge collection of similar technologies and products, and as a result it's hard for people to understand the security threats and how to deal with them," he claims. "The expectation is often that you just type in your credit card details and the provider will act in your interests."

This is certainly not the case though, Lyne believes. Before signing a contract with any cloud vendor, he continues, it is essential to ascertain where responsibilities lie with each party in the provider/customer relationship. "It's critical that you create a contract with the provider that outlines what

security controls they will run, how they will notify you if there is a breach, how they will monitor developing compliance regulations and your exit strategy in the event they do not perform," he remarks.

Maher Jadallah, MEA regional manager at Sourcefire, a developer of network security products, advises that businesses thoroughly audit any potential cloud vendor before agreeing to procure any service. "You should have a clear picture of their security infrastructure and policies; the level of security training their personnel receive; their physical access controls; their patch management, vulnerability assessment, and logging policies; and their firewall and intrusion detection and prevention systems," he explains. "If the cloud provider outsources security to another vendor you need to understand their contractual obligations."

The security considerations do not end after selecting a cloud provider. There are several IT infrastructure surfaces that require intrusion protection, reckons Mashood Ahmad, regional MD, Ciena Networks, with one of the most obvious of these being the network.

The fact that cloud computing services transfer data from an organisation's internal infrastructure or data centre to a cloud vendor's infrastructure via the public internet complicates the security process. "IP (internet protocol) security breaches are an important and frequently recurring threat - failing to protect the network is therefore a fundamental mistake," Ahmad says. "IT and network managers need to take the entire data path

into consideration when developing a security strategy." Methods for reducing the likelihood of data being accessed while travelling between the customer's and cloud provider's infrastructure include implementing a virtual private network (VPN) and data encryption at the source, adds Ahmad.

At all times,



James Lyne: cloud definitions equal cloud confusion

Confusing definitions of the cloud do not help security matters, says Sophos's James Lyne

the keys to this encrypted data should remain with the customer, and never with the cloud vendor.

The multi-tenant nature of public cloud services, which host numerous clients' data within the same physical infrastructure, also poses security risks. That customers often have no idea who their cloud is being shared with, and for what purpose they are using it, is a consideration businesses must bear in mind.

"The multitenant nature of public clouds means that you may be sharing infrastructure with a completely unknown set of other parties," warns Sourcefire's Jadallah. "Your neighbors could be independent hackers or those employed by competitors, organised crime, or others looking to gain access to your most critical data."

Abdulrehman Ubare, head of technical operations at UAE-based managed services

provider eHosting DataFort, says that this multitenancy can mean that hackers who gain access to one business's resources, may also be able breach the assets of another organisation that they share cloud infrastructure with. "Cloud computing uses shared resources similar to network infrastructure, such as shared switches," he explains. "In such cases there is a possibility of seeing VLAN (virtual local area network) 'hop attacks' where customer X can access customer Y's resources by bypassing VLAN boundaries."

To effectively safeguard against such threats, Ubare believes, organisations should ensure that their cloud vendor implements effective access control policies within shared infrastructure where possible.

OUT OF CONTROL

According to Sophos's James Lyne, some of the networking

risks associated with cloud computing are exacerbated in the Middle East. For one, he highlights that local regulations on data are not developed to the extent they are in the West. "The Middle East as yet has a relatively light legal framework for these kinds of issues," he says. "This can lead some to be lax in following best practices."

applications and services hosted in the cloud, then organisations must also scrutinise ways of securing them. An added complexity is that these devices will often interact directly with cloud providers over the public internet, rather than through a corporate network or wide area network (WAN). Security must take into account the different

technologies are brought up to date to protect the mobile user and to provide widespread platform support," Lyne believes. "Security technology deployed here needs to work whether the user is in or out of the office, or at home, ensuring that a business's reputation and data is consistently protected."

There is one concern over the cloud that is universal, according to Nick Black, regional technical manager at security provider Trend Micro. He says that it is natural for businesses to feel

uncomfortable when it comes to moving their data outside of their organisation, and to a third party, which the move to a cloud provider necessitates.

"There's a separation anxiety people get when they move data," he observes. "Take a bank, for example, and its customer database, which shows how much money each of its customers has. Would a bank be confident right now to move that somewhere else? Somewhere it may not physically even know where that is?"

Black echoes other security experts in highlighting the various attack surfaces that exist in the cloud-enabled organisation.

"There are technologies that are available that secure the whole concept though: that secure the network, to the endpoint, to encrypting the data so that when you do terminate the service, the data is not available to anyone else."

Whether businesses in the region are ready to trust these solutions though, is another matter that must be resolved. **N**



Customers should fully investigate their cloud vendor's security measures, claims Sourcefire's Maher Jadallah

"You should have a clear picture of the cloud provider's security infrastructure and policies," explains Sourcefire's Maher Jadallah

Lyne also points to the recent explosion of smart, mobile devices being used by businesses in the region. If these are being used to access

software platforms devices use, such as Apple's iOS and Google's Android.

"It is critical therefore that security policies, practices and

Public exposure?

Distinctions need to be drawn between private and public clouds, says Bashar Bashierreh, regional director, Fortinet Middle East.

"The private cloud is in fact just a highly virtualised data centre of networks, servers, applications and even security. For example, high-performance firewalls, once only available as a dedicated network hardware security appliance, can be manipulated as multiple virtual instances like any other hardware-based infrastructure component, allowing scalability and centralised management. The benefits of virtualisation now apply to your entire network infrastructure.

"One of the potential risks of private cloud comes from the rule sets complexity of a multitenancy environment, defining routing and access to domain resources. Those are critical to prevent unauthorised access to private information.

"In the public cloud, 'Security as a Service' is one of a host of services that promise to better resource IT departments on tap. Cloud providers can drive these resources with immediate flexibility and at compelling price points, thanks to their own use of virtualised security but they must provide security control transparency to their end customers if they want to see adoption.

"One could argue that public clouds can be more exposed to internet attacks because cybercriminals can yield higher benefits since cloud providers are connected to many corporate networks, representing a good entry point for distributed attacks. However, one thing to keep in mind is that the security controls of cloud providers are often stronger than the internal ones of a private enterprise, especially with SMB companies."