

Cloud security basics: A guide to ensuring cloud security, today

Everyone's talking about cloud computing these days. However, there is a significant security risk that increases with the explosion of cloud computing adoption.

Cloud computing makes certain applications or infrastructure available on an as-needed basis. It's infinitely easier to manage for businesses who may have otherwise struggled with the capex investment, implementation, ongoing management or scalability. However, most implementations of cloud based services are not properly protected and are generally easy to hack in to, which in itself is worrying, but what makes this a BIG concern is that most advice you find on the internet does not secure your cloud TODAY. Most advice relies too much on "future" solutions such as OpenID or SAML. This paper provides advice and solutions to secure your data immediately.

What the hype's about

Both the National Institute of Standards and Technology (NIST) and the Cloud Security Alliance define the cloud "as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." The pay-as-you-go services benefit any size business across the board. Businesses pay on a utility-type consumption basis.

Industry concern

Industry experts express concern that businesses 'jumping on the bandwagon' of cloud computing's impressive benefits may not be taking the appropriate necessary review of their own security policies. Security expert and ex-ethical hacker, Jason Hart is concerned that moves to a virtual world using cloud-based technologies could end up being a virtual disaster – unless businesses act today. "I am concerned that many of the vendors and providers are only paying lip service to security and are more caught up in the hype than the reality of the situation. Every service or platform I look at is still only secured by a traditional password – and that is not sufficient to keep hackers at bay – as recent attacks on Twitter have shown", said Hart, now Senior Vice President - Europe for CRYPTOCARD, the Passwords-as-a-service company.

Not just for smaller businesses

Adoption of cloud computing is accelerating, and not just within smaller companies. Rentokil Initial and Jaguar Land Rover have each recently announced the move of large numbers of employees to Google's hosted office applications suites, a combined total of 50,000 employees. Rentokil Initial's rollout of cloud based services to 35,000 employees comprises the largest to date. They will use the web-based communication and collaboration suite across fifty countries. Up to 15,000 of Jaguar Land Rover's employees will now have the ability to access email and calendar services from any Internet connected device through Google Apps Premiere Edition. Each business sited significant cost savings as factors in the decision.

Future security solutions are remote

Because cloud computing represents a revolution in IT management, this paradigm shift makes it even more critical that businesses review security policies now. With more than 223 million records containing sensitive material compromised since 2005, according to Data Breach DB, a clearing house for data breach information, and the more recent attacks on Twitter in July 2009, businesses must make security a priority. Hart asserts, "The key recommendations from advisory bodies, councils and forums is to look to Federated ID and SAML – but these are too far away from commercialization for them to stop today's threats. So, I would strongly recommend business take some simple and immediate steps to counter the threat of ID theft and hacking."

Social networking and the risk to security

Businesses are realising some value in employee access to Web 2.0 social networking sites like LinkedIn, Facebook and Twitter, and not necessarily blocking access from the company network. Increased use of social networking sites massively accelerates the associated security risk. While social networking sites themselves do not represent a threat, the risk is social engineering based on the information hackers glean from these sites.

Research shows that 40% of staff utilise the same password for multiple accounts – webmail, social networking and accessing your network, according to Ponemon Institute's survey, Trends in Insider Compliance with Data Security Policies 2009. This means your network is only ever as secure as the weakest password. Static passwords provide the easiest way into your network for hackers, attackers, shoulder surfers, key loggers or even a curious neighbour.

Impacts of a changing economy

Aside from recent and ongoing security breach concerns, the economy is changing the way businesses work today. This means more workers are accessing confidential information from more places outside the typical business setting using remote access services (RAS), and from more types of devices. Implementation of RAS with an ondemand managed authentication service can reduce the need for unnecessary travel, as well as provide a basis for business continuity in the event of disaster driven forced home working.

Now is the time to act

Businesses have a duty of care to ensure their own 'borders' are protected, and the nature of the 3rd party relationship inherent in cloud computing means in-house security policies need an immediate review with the adoption of cloud computing in any form. Even businesses reluctant so far to adopt widespread cloud computing may not, in fact, realise they're already using applications that reside in the cloud.

Clients and applications such as Skype, MessageLabs, Salesforce, Microsoft Online Services, Facebook, Twitter and LinkedIn are cloud based. The time to act is now, and the steps to take are simple.

Six steps to take now to ensure your security in the cloud

Hart's recommendations are simple and easy to implement.

Many of them utilize cloud based solutions to reduce cost and management headache:

<p>1. Teach ALL users "Safe Internet Skills"</p>	<p>Staff using the internet for work should be educated not to engage in risky behaviours – sharing or writing down passwords, responding to phishing emails with confidential information, downloading applications and documents without verifying the source.</p>
<p>2. Perform a DETAILED vulnerability assessment - Make sure each "border" is protected</p> <ul style="list-style-type: none"> • Data centre • Access points • Devices • Suppliers 	<p>Review each point into/out of the network to expose where an attack could breach a border – a vulnerability assessment and testing tools can confirm weak points. Take immediate steps to close the gaps in IT security, investing in those that pose the greatest risk to the business. Implement routine vulnerability assessments as a standard part of security policies. Ensure employees and contractors adhere to internal security policies.</p> <p>Verify security policies of all suppliers.</p> <ul style="list-style-type: none"> – One in five IT managers believe supplier equipment is less secure than their own, but continue to outsource. – Only 64% of IT managers in medium-sized businesses expected suppliers to have formal security procedures and policies in place. - NCC Group report
<p>3. Use current Anti-virus software on EVERY device – All company devices, servers and home computers</p>	<p>Don't be tempted to cut the budget here. Protecting against threats with automatic scans, updates and outbreak alerts costs significantly less than what companies spend in remediation following a cyber-attack.</p> <ul style="list-style-type: none"> – One in five mid-size organisations had an attack that caused a loss in revenue in the last year – 70% of businesses estimated some chance that a severe data breach could put the company out of business - McAfee Labs report
<p>4. Use a firewall at EVERY point – Block unused services, ports and protocols</p>	<p>Today's firewalls protect against both internal and external attacks, typically preventing unauthorized access or users from gaining access to the network. The right firewall implementation ensures your mobile workforce has access to key resources with a smooth exchange of data, keeping productivity up while maintaining network security.</p>
<p>5. Use encryption and certificates for ALL sensitive information – VPN, Secure e-mail, portable devices</p>	<p>Encrypt all data, especially on portable devices. Even with security policies in place, an alarming number of employees disregard security policies and procedures. One of the highest threat concerns the transfer of company confidential information onto a USB memory stick:</p> <ul style="list-style-type: none"> – 61% of employees say they do it – More than 43% of respondents admit they have lost or had stolen a portable data device. <p>Ponemon Institute's survey, Trends in Insider Compliance with Data Security Policies 2009.</p>
<p>6. Deploy strong authentication for EVERY remote user - 8 character password, strong PIN, separate token</p>	<p>Secure your data from the unseen threat of hacking. Your network is only as secure as the weakest password, traditional passwords have been around since the 1950's and were designed for much less complex networks and applications.</p> <p>Two-factor authentication validates those accessing the network using a One Time Password (OTP) that is good for one authentication event only, making capture by a hacker useless. The combined two factors of something you know (a PIN) and something you have (a token or card that which provides the unique OTP) eliminates the ease with which traditional passwords can be compromised.</p>

Not just market hype

Richard Carty of NetShield, a UK managed services provider, agrees with this advice. “Our customers have a very real challenge in implementing cloud based and managed services – and our consulting team advise any customer to conduct a comprehensive audit of their service providers policies before they deploy. We have been delivering managed security services for the past 10 years and are keen to ensure that every one of our customers heeds this advice.”

There has been a lot of recent hype from vendors and service providers about what technology is coming in the future. However, existing security risks mean there is a need for these solutions today. Gary Collins, CTO of On-Line Services provider Intercept-IT says “Our on-line services are delivered with two factor authentication as part of the package today. There is no question that any cloud based service needs to be based on solid and secure foundations – and businesses are advised to act today. We believe Jason’s advice is not only critical but delivers a solution to today’s need – and not one of market hype.”

CRYPTOCARD has 20 years experience in IT security, and counts recognised industry experts amongst its staff. Commitment to innovation in line with market threats and trends has won CRYPTOCARD several key industry awards for their portfolio of cutting edge products.

CRYPTOCARD Europe

Tel: +44 870 7077 700

CRYPTOCARD North America

Tel: +1-613-599-2441

info@cryptocard.com www.cryptocard.com

CRYPTOCARD