

Cloud Computing –what are the security issues?

Cloud computing is definitely the fashionable topic for 2009. However, there is a distinct lack of visibility into security in cloud providers, with commentators saying that most appear to want customers to treat them like a black box. “You can’t know where your data is, you can’t prove that it’s being protected and you can’t know who’s accessing it.” according to Robert Richardson, director of the Computer Security Institute. This is clearly at odds with recent legislation which requires all of these things.

The risks are considerable, with the potential for exposure of customer data, credit card details, personal information, business plans and more. The impact could range from loss of competitive advantage to criminal prosecution and loss of shareholder confidence.

With many large organisations struggling to come to terms with legal and contractual obligations for in-house security, as well as the downturn in the economy, the temptation to outsource into the cloud is obviously considerable. However, outsourcing applications and data management does not mean you can outsource your responsibility for security.

In a situation where you don’t know where your data is stored - even which countries are involved - how can you comply with Data Protection legislation? You have no idea who has access to your data, and whether or not the provider’s staff have been vetted. You don’t know how well your data is segregated from other users. Is the data encrypted? How is it backed up, how often and where? These are all questions that should be answered before contracts are signed, yet they may not be considered at all.

Amrit Williams, past research director at Gartner, made this succinct observation on his blog: “When we allow services to be delivered by a third party, we lose all control over how they secure and maintain the health of their environments - and you simply can’t enforce what you can’t control. The ‘experts’ will tell you otherwise, convince you that their model is 100 per cent secure and that you have nothing to fear. Then again, those experts don’t lose their jobs if you fail.”

Based on my experience as an ethical hacker, I spent a few minutes brainstorming potential threats to your data in the cloud. The most obvious were these: attacks against the provider’s web site, unauthorised access by provider’s staff and contractors, malware infection, denial of service attacks, transparent access by other users, loss of backup media, loss of unencrypted data on laptops and memory sticks, wireless hacking at the provider’s site and interception of data in transit. Since we have no idea how your data will be protected, any of these attacks may be viable.

If a criminal (or a competitor) is going to target your data, then they’re going to take the route that combines the highest probability of success with the lowest risk. Successful attacks don’t focus on just one vulnerability - exploiting a combination of technical, physical and human weaknesses is standard practice in the criminal underworld today. Once you outsource to the cloud, you lose the ability to control or monitor these attacks, and you introduce new vectors that a criminal can manipulate. The more parties are involved, the greater the risk. Impersonating a client or their agent and gaining unauthorised access to data becomes more likely, as does the opportunity for data interception.

With all these risks, it becomes essential to conduct a thorough review of the provider’s security to ensure good governance. This means inspecting their information security policy and procedures against proven standards such as ISO 27001. It means asking for proof of their staff vetting and management processes, as well as their technical infrastructure. They

Cloud Computing –what are the security issues?

must be able to assure you of their data security controls, such as encryption of data, both in transit and at rest. They should be able to demonstrate that they undertake regular, independent audits and penetration tests and be willing to share the results with you. Your contract should also give you the right to conduct audits and tests of your own.

Only when your security team and your auditors are happy with the results of your review, and all the necessary controls are embedded in your contract, should you consider entrusting your data (and your customers' data) to a third party "somewhere in the cloud".

First Base Technologies is exhibiting at Infosecurity Europe 2009, the No. 1 industry event in Europe held on 28th – 30th April in its new venue Earl's Court, London. The event provides an unrivalled free education programme, exhibitors showcasing new and emerging technologies and offering practical and professional expertise. For further information please visit www.infosec.co.uk

Peter Wood is Chief of Operations at First Base Technologies, an ethical hacking firm based in the UK. Peter founded First Base in 1989 and has hands-on technical involvement in the firm on a daily basis, working in areas as diverse as social engineering, network penetration testing and skills transfer. Peter is also a world-renowned speaker and security evangelist.

Peter Wood
Chief of Operations
First Base Technologies
Town Hall Chambers
High Street
Shoreham-by-Sea
BN43 5DD
UK

Tel: +44 (0)1273 454525
Fax: +44 (0)1273 454526
e-mail: peterw@firstbase.co.uk

www.firstbase.co.uk
www.white-hats.co.uk
www.peterwood.com