From: www.cio.com

How Secure is that Cloud Vendor? 7 Basics

– David Taber, CIO

January 26, 2011

Cloud computing security is an incredibly broad (and deep) topic, so I can only scratch the surface in a short article. Even so, let's try to get the basics under control.

Cloud Security: Ten Questions to Ask Before You Jump In
Defining Cloud Security: Six Perspectives

The first order of business is making sure we're talking about the same thing. Some cloud vendors try to blur the lines between security, reliability, and disaster recovery/business continuity. While all these are important attributes, it just confuses the conversation. So let's stick with the standard definitions in this overview.

1. Let's Get Physical
In on-premises systems, Job 1 of security is to make sure that unauthorized people don't get physical access to the machines. If someone can connect foreign hardware, reconfigure the system, or control the system boot cycle, an awful lot of security is out the window. In a cloud-based service, you don't have to worry about this on the server side — that's the vendor's job. While there have been occasional breaches of cloud services over the years, established cloud vendors have pretty tight operations groups — and most of them treat their internal security procedures as highly guarded trade secrets. Which means you won't be able to get much info to evaluate them. With a reputable vendor, it's safe to ignore this issue.

2. Identity Crisis
The next item that must be handled is identity across clouds. The first things to look for are in the area of authentication and authorization: password strength, IP range blacklists/whitelists, login hours, two level authentication...all the stuff you're used to with on-premises systems. Most cloud vendors should have this covered, at least through add-on features or modules.

And of course, there's the too-often-neglected issue of privilege revocation. While this is more a process issue than a systems one, look for features that prompt the administrator (or automatically warn of users who likely need revocation) to make for a tighter ship.

The other side of the coin is making the authorization process less annoying to users: SSO connectors and delegation infrastructure are needed for any practical multi-cloud applications. User account or ID anonymization/obfuscation are particularly important if your applications need to span suppliers or channels in the supply chain.

3. Encryption
Encryption is an obvious requirement for cloud applications, and https is the baseline for all user logins and integration connections. Many cloud applications, however, are not built to have the data encrypted within the cloud. Indeed, in some cases it's not even possible to have the cloud data stored in encrypted form. As this poses risks for customer privacy, corporate snooping, and even Fourth Amendment protections, ask your cloud vendors about internal encryption and push for it in their roadmap presentations.

4. ILP/DLP
As I wrote in an earlier column, information loss protection (aka data leakage prevention) is a critical issue for business applications. Every year, 80 million consumer identities in the U.S. become compromised due to accidental losses and deliberate attacks. Even if you like WikiLeaks, losing control of business information is something to worry about.

In cloud systems, there are two major risk areas for leaks. The first category is a breach within the

cloud vendors — something you have little control over (other than vetting vendors). But you can at least demand as part of your cloud vendor SLA that they notify you of any breach that affects your data.

The second category of breach you do have control over: loss at the end-point. This requires add-on software or hardware for each server, PC, and mobile device that presents or processes data from your cloud application. The goal is to make sure that only authorized data transfers occur, and they must be regulated down to the device and file/object level. Further, use of file encryption and auto-erase (upon loss of control of the device) are required, particularly if your organization has a large field force. While general purpose ILP/DLP products are a good start, there are now some startups offering solutions tailored to the specific needs of cloud-based software.

5. Privacy
Depending on the industry and location of your business, there is an amazing array of privacy acronyms that your cloud application will need to comply with: PCI, GLBA, CA1386, HIPAA, FERPA, Directive 95/46/EC...the list seems endless. The first order of business is nailing ILP/DLP: you can't comply with any privacy standard if the information has leaked out of your organization.

The next step is to ensure that your cloud vendors are compliant with the regulations, or at least have a safe-harbor certification. While many cloud application vendors have achieved this, there are some categories (notably cloud-integration vendors) whose current generation of services probably can't be certified.

As compliance in many privacy areas will require process changes on your part, don't think of this as a problem you can fob off entirely on the vendors. I hate to say it, but "consult your attorneys."

6. Audit
Audit trails — for login history, administrative actions, and data changes — are an essential ingredient to security. While an audit trail won't stop a breach, it provides critical forensic evidence about what occurred and how to conduct a remediation.

While backups or archives are essential tools, they are not a substitute for a formal audit trail (who changed what when). Make sure that your cloud vendor offers an option for logging before you sign up for the service, and make sure that you've turned on that option from day one. You probably won't be able audit every field's change, so make sure to choose the ones that are the most sensitive and relevant. Finally, make sure that the audit trails are themselves backed up (onto your own local media), as they may disappear from your system after a few months. Recovery of these audit trails from within the service can be hugely expensive.

7. Denial-of-Service Attacks
Denial-of-service attacks are likely to be a permanent fixture. While they are unlikely to target just your organization, when cloud vendors come under attack your business continuity can be affected. Like with disaster recovery, you need to know what remediation strategies your cloud vendors have in place, you need to negotiate for an SLA covering service recovery time.

The Big Kahuna
When it comes to cross-cloud computing, the big issue is "access control." It's so big, it deserves its own article — so see you next week.

David Taber is the author of the new Prentice Hall book, "Salesforce.com Secrets of Success" and is the CEO of SalesLogistix, a certified Salesforce.com consultancy focused on business process improvement through use of CRM systems. SalesLogistix clients are in North America, Europe, Israel, and India, and David has over 25 years experience in high tech, including 10 years at the VP level or above.

Follow everything from CIO.com on Twitter @CIOonline.