Sunday, December 11. 2011

Why One Should Avoid The Cloud Hype

This entry has been updated (Feb 20, 2014)

Cloud computing is nothing more than a marketing term for technologies that provide computation, software, data access, and storage services that do not require end-user knowledge of the physical location and configuration of the system that delivers the services. (Source - Wikipedia)

Cloud computing is nothing new, it has been around for decades. Email or Web Hosting anyone? The term Cloud is used as a metaphor for the Internet, based on the cloud drawing used in the past to represent the telephone network, and later to depict the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents, but in recent times, some marketing hero decided to come up with a new hype, and like all techno weenies, the media picks up on it, these stormy cloud times are rather funny, but sad.

Richard Stallman of the Open Source Software Foundation summed it up nicely in an interview with The Guardian â€œItâ€™s a trapâ€¦ Itâ€™s worse than stupidity, itâ€™s a marketing-hype campaign.â€•

Here at home in Australia, organisations investing in off-shore cloud services could find themselves on the pointy end of legal action should the privacy of Australians be breached as a result, Victoria's acting Privacy Commissioner has warned

For companies, its a privacy nightmare, you may not even know which country your data is in, and chances are their privacy laws wont be as tough as local laws, then there's the inherited dangers of dealing with American firms, The U.S. Patriot Act requires all U.S. incorporated businesses to comply with demands for information, even if your data is on that firms non U.S. located servers. The Canadian Government has made it unlawful to host Government material in the U.S. explicitly because of The Patriot Act and many other Governments and companies around the world are thinking twice about using the U.S. Cloud hosting. Australians are fairly lucky in respect to having tough privacy laws, but all that goes out the window too when hosted in the U.S. and likely other overseas content providers, as well as any U.S. incorporated firms based within Australia, yes, this could mean Microsoft, Google, Amazon et cetera.

Then there is data integrity, what sort of network is your data on, what is the competency of their programmers, their server administrators, what sort of contingencies do they have to keep your staff working, or your clients happy in event of failures, we've all seen the failures of Google and Amazon clouds multiple times in past year or so, even Microsoft cloud services had a pretty big failure earlier this year as well.

This post was started in draft stages on Dec 5, since it always takes me a few days to be happy enough to finalise it ready for publishing, I must have known something (wish my lotto entries had as much success as my other sub conscious predictions heh) by not getting back to it for a few days longer this past week, because on Friday, Telstra Big Pond (Largest Australian Service Provider) had a massive Privacy Breach in its systems for customer self service that saw it, and all Email disabled for close to 24 hours, It affected a large number of people "The exposed site offered customer service-level access to customers of Telstra bundled products. Information accessible included a veritable feast for identity theft: bundle information, telephone numbers, users names and addresses, logins and passwords" - surprisingly what most did not know is that Telstra outsource this service, yes, you guessed it, to the stormy Cloud, how stingy can they get, not using their own infrastructure, to quote The Register The site is not actually hosted on a Telstra domain: itâ€™s a cloud-based service on the custhelp.com domain operated by RightNow Technologies. The equally scary thing is, apart from being reported on two online media outlets, the SMH and the Australian, lets face it who the hell reads either of those? Maybe half a chance for the SMH if you live in NSW, but what about the rest of the country? There were no reports in the mass media, ie: Radio and Television news, certainly not on the more popular commercial stations, and still hasn't been, very nice job of hushing things up appears to have been done. It just goes further to show why this marketing thing called Cloud, is a load of rubbish and has very severe security implications for all who use, or contemplate using it.

World renown security expert Kevin Mitnick has had much to say on Twitter about this, but one of Kevins recent tweets sums it all up nicely:

With the Cloud, security has been, and continues to be, a real concern. It might be a convenience, but is it really in the long run? Businesses (in fact all) data protection should be of the highest concern, and the only way you will know it is secure, is by housing the equipment in-house where you can separate the intranet from the big bad internet, and have direct and immediate control of what code developers do. It's like that file server with all those highly confidential contracts on it being plugged into the Internet, with no access control lists, all there for the taking.

What about if you have a dispute with the host provider and they suspend your service? How long will your business last if they deny you access to your own data?

Cloud is nothing new, with what these marketing folk interpret as The Cloud today, is mostly used in cost cutting, with a very high degree of risk. This risk is acceptable in Web Hosting, Online shopping carts and so on, everyone knows what to expect because it's been around for well over 20 years, and everyone's doing it, but, it's a completely different thing when it comes to putting businesses operational material on an Internet based service, this is very very dangerous, and all businesses should conduct a fine detailed risk assessment, including your insurance and banking, and so on, you might find your premiums increase, your bank manager might consider it too risky to approve your next loan, and you might be in breach of the law if your move to the Cloud makes you non PCI DSS compliant.

Simply put, leave the real Cloud (Internet) for what it was designed for, transmission of information (ie: Email, Web, et cetera) and keep your business data on an air-gap (no way possible to reach Internet) Intranet, that way the security is assured. Your customers don't care about buck passing, like for example, RightNow, they have no contract, no service agreement, no nothing with them, they have those things with you, or in our example, Telstra. It is your name that will be damaged, now that might be acceptable to an organisation of Telstras size, and lets face it, they don't care too much for what anyone thinks about them anyway, but ask yourself this, are you big enough for any backlash? Most would have to say no, especially if you're concerned about your company image, remember, word of mouth can do damage as well as good, most people will research you online before considering doing business with you.

Privacy waived by carriers

Australias Telstra agreed more than a decade ago to store huge volumes of electronic communications it carried between Asia and America for the U.S. Government

â€¢ Microsoft helped the NSA to circumvent its encryption to address concerns that the agency would be unable to intercept web chats on the new Outlook.com portal;

â€¢ The agency already had pre-encryption stage access to email on Outlook.com, including Hotmail;

â€¢ The company worked with the FBI this year to allow the NSA easier access via Prism to its cloud storage service SkyDrive, which now has more than 250 million users worldwide;

â€¢ Microsoft also worked with the FBI's Data Intercept Unit to "understand" potential issues with a feature in Outlook.com that allows users to create email aliases;

â€¢ Skype, which was bought by Microsoft in October 2011, worked with intelligence agencies last year to allow Prism to collect video of conversations as well as audio;

â€¢ Another Dangerous U.S. Govt Act is the Stored Communications Act, and little known fact that classifies all data older than 180 days as abandoned, this means it can be accessed at any time, without warrant or just-cause, or any reason at all, so if you thought those messages on gmail or hotmail/live, or your data in Googles Drive or Microsofts Skydrive, which is over 180 days old, are covered by any privacy laws, then think again, the U.S. Govt interprets this data as abandoned and can read to their hearts content.

Updates!

In what can only be described as a shocking decision, Bigpond customers emails are now to be stored in the cloud. The horrifying thing about this is, Bigpond users although warned of this outsourcing, were not told the data will not be stored in Australia, but likely in either Singapore, or the U.S.A., both of which have far relaxed privacy laws compared to Australia, and as indicated in my comments in my The-Internet-and-Legal-Jurisdictions article, you can see how far the

U.S. agencies will go, but it will not be much better in Singapore!

Time for Bigpond'rs to consider if they want to remain in the muddy puddle or move to brighter and greener pastures.
Reference: ITNews

I trust Telstra will no longer use the add that involves the lyrics I am, we are, Australian, since they have shown what they think of Australia.

And a new warning to rethink where you host anything might be even more important now to consider given the U.S. FBI wants legal back doors mandated into websites that will of course see non U.S. citizens also targeted with this stealth secret police state mentality the U.S. Govt agencies have as well as their own citizens.

Even a very famous hacker from years gone by turned security consultant, Kevin Mitnick, does not trust the cloud.

Update:
Recently, Amazon has shown why not even they are all that reliable for your business..
Amazon Web Services sometimes replaces the hardware virtual servers run on and switches those servers off without elegant or accurate notifications of whatâ€™s about to happen.

A trawl through AWSâ€™ support forums suggests that the company isnâ€™t switching off servers without notifications every day, but threads pop up quite regularly in which users complain about servers disappearing.

Full report courtesy of The Register

Update2:
Yet more Amazon outages, this time 20 hours for major clients during Christmas 2012, yet another one in the ever growing number of outages, where the smaller players, as in most local Web Hosting providers, or in-house data storages, don't experience so much drama.

Update3 - 2013
A routing fault on the SingTel network has caused four days of mail issues for subscribers to Microsoft Office 365, once again (losing count now) highlighting yet another failure by using offshore cloud services.

The problem was first reported in the Microsoft Office 365 Community forum on January 5, 2013, with users noting that they could not reach the servers hosting their Outlook mail and that they had received retransmission errors.

Read more about yet another offshore cloud screwup

Update Aug 9, 2013

In what can be described as a sad day for Email providers, Lavabit has now, at least for the time being closed, due to secret efforts of the US government trying to spy on its users, with a stern warning from its owner

This experience has taught me one very important lesson: without congressional action or a strong judicial precedent, I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.
Ladar Levison
Owner and Operator, Lavabit LLC

Update Aug 15, 2013
Google's lawyers freely admit your Gmails are theirs, and not yours.

Consumer Watchdog has unearthed a brief filed by attorneys for Google saying Gmail users have no reasonable expectation that their communications will be kept secret.

â€œGoogle has finally admitted they donâ€™t respect privacy,â€• said John M Simpson, Consumer Watchdogâ€™s Privacy Project director. â€œPeople should take them at their word; if you care about your email correspondentsâ€™

privacy donâ€™t use Gmail.â€•
read more at Siliconrepublic

Update Oct 15, 2013
Telstra Dumps Offshore Cloud Email Hosting.
Telstra has quietly shelved a major deal with Microsoft that would have seen it migrate 4.2 million email addresses to offshore hosting facilities.

Update Feb 20, 2014
In another Google cloud screwup involving serious breach of privacy, accessing third parties Google Drive files

Attackers can access a user's Google Drive files and record them through their webcam by tricking the user into clicking hidden links, a researcher found.

.. Google fails to verify whether a user is authorised to view the sensitive thumbnail
Hell, they even allow unauthenticated access to the thumbnail!

Read more of the yet another cloud blunder at ITnews.

Posted by NoelB at 16:02