Cloud Security – Risks and rewards

Some security implications of cloud computing

Taz Wake
Halkyn Consulting
Security & Risk Management Specialists

Cloud Security – Risks and rewards

There are a lot of business advantages to making use of the cloud for your IT requirements. The ability to make use of shared resources can significantly reduce costs, capital expenditure and simplify your maintenance and upgrade requirements.

Even for home users, there is a strong trend towards making use of cloud services – Gmail, GoogleDocs, DropBox etc. are all examples of what the cloud can offer. With the advent of devices like the iPad and the Google Chromebook more and more people are storing significant amounts of their data in the cloud.

Despite the obvious benefits, there are also significant risks present with any form of cloud service.

Some risks are obvious, but others may get hidden beneath the sales pitches that the cloud providers will bombard you with. Add to this the fact that few businesses have sufficiently trained staff or even access to enough information to make sensible, business oriented, risk decisions and it is obvious that lots of organisations are simply hoping for the best.

One of the rarely considered risks is what happens if someone who is also part of the shared resource you are has problems. Most hosting providers (importantly, **not all**) will have backups and segregation mechanisms in place to prevent a broken application taking everything down but what happens if one of the companies on your shared platform breaks the law?

While this might be an unusual situation, it happened early today[i]. In the US (where the majority of the cloud providers are based), the FBI raided a data centre to seize servers as part of an on-going investigation. It appears that the servers were part of a virtualised platform, which meant that the FBI ended up seizing systems that were servers for several other companies.

From the New York Times[ii]:

> The F.B.I. seized Web servers in a raid on a data center early Tuesday, causing several Web sites, including those run by the New York publisher Curbed Network, to go offline.
>
> The raid happened at 1:15 a.m. at a hosting facility in Reston, Va., used by DigitalOne, which is based in Switzerland, the company said. The F.B.I. did not immediately respond to a request for comment on the raid.
>
> In an e-mail to one of its clients on Tuesday afternoon, DigitalOne's chief executive, Sergej Ostroumow, said: "This problem is caused by the F.B.I., not our company. In the night F.B.I. has taken 3 enclosures with equipment plugged into them, possibly including your server — we cannot check it."

Without knowing the specifics of why the FBI raided the data centre (or the terms of the warrant used) it is hard to go into that part of the event; however it is fairly normal for law enforcement officials to want to collect as much hardware as possible so that any resulting forensic images have as much value as possible.

Further on in the article is this comment:

> DigitalOne provided all necessary information to pinpoint the servers for a specific I.P. address, Mr. Ostroumow said. However, the agents took entire server racks, perhaps because they mistakenly thought that "one enclosure is = to one server," he said in an e-mail.

This points to the crux of the problem here. Even if the police are targeting a specific system mistakes happen and it is rarely technical people on the task.

When it comes to hosting your systems in the cloud, you **have** to have a documented, detailed risk management plan in place and while you can't be expected to cover every eventuality you **absolutely must** have a backup plan for when "unforeseen events" take out the cloud provider.

It is also worth, as part of your risk assessment process, checking out the terms and conditions of the contracts you have with your cloud provider. If your systems are taken

down (in this manner or in any other) do you have legal recourse to recoup any losses? Obviously, the more business you do online, the more important this is.

If you want to discuss anything related to cloud security risks, or would like to find out how Halkyn Security Consultants can help your business then get in touch today. Our security experts are experienced in all aspects of security, including physical protection, staff security, awareness and training, risk management and business continuity planning. We will never try to sell you services you don't need and will always ensure you get the most cost effective advice possible.

About Halkyn Consulting

Halkyn Consulting Ltd is a specialist security consultancy based in North Wales, experienced in providing security advice to local, national and international clients including government agencies, multinational corporations, small businesses and homeowners.

For more advice on how to properly use passwords or any other questions you may have related to security and protecting your home, business or other assets, you can reach Halkyn Consulting at www.halkynconsulting.co.uk or info@halkynconsulting.co.uk.

[i] 22 June 2011, when this article was initially published.
[ii] http://bits.blogs.nytimes.com/2011/06/21/f-b-i-seizes-web-servers-knocking-sites-offline/ – retrieved 22 June 2011.