

Cloud computing & small businesses – security pros and cons

Written by Dan Conlon, Engineering Director, Trend Micro

As we've seen, there are many advantages for small businesses in using cloud computing. It enables you to do more with less, accessing critical business applications without the need to pay for ongoing maintenance or upgrades. It also enables services such as Facebook, LinkedIn and Twitter which can offer you unique ways of reaching out to customers and potential employees.

SB's under attack

However, small businesses, like their larger counterparts, are under attack on a daily basis. Data-stealing malware like the infamous ZeuS, is rife online, with attack kits readily available for purchase on internet forums. The criminals could be after your customers' banking and other personal data, or even your intellectual property, all of which can be easily traded on the same online forums.

Small businesses are being assailed from all sides. There are targeted email scams designed to trick the user into clicking on a malicious link or opening an attachment which could trigger a malware download for example. Then there are infected web sites, often legitimate sites which have been hacked, and all it takes is for an employee surfing the web with a vulnerable machine to visit those sites to be immediately infected.

The same threats exist on social networking sites, with malicious links and rogue applications popping up across sites such as Facebook with the intention of stealing your data.

Is the cloud safe?

So what are the dangers of cloud-based computing systems? It's important to remember from the outset that cloud computing in the small business environment may well be a less risky choice for firms than keeping all their IT operations in-house. Many people feel inherently ill-at-ease with having customer and staff data, financial records and their IP leaving the premises and stored off-site in their cloud provider's data centers. But this knee-jerk reaction shouldn't mask the truth that in many cases you would be outsourcing to a more secure environment.

Imagine, for example, that you can't afford to run a central server in your business, meaning all customer, financial, IP and other data is stored on your or your employees' laptops or USB drives. It's not only a less efficient way of working but it increases the chances of data loss, and the regulatory financial penalties, loss of business and more importantly reputational damage that will ensue.

Compare this with a reputable cloud provider which is fully regulated and certified by independent standards bodies to a high degree, and as a result would be protected by state-of-the-art security systems preventing data theft. Back-up is continuous and if you lose your machine there's no need to worry because all the data is stored in the service providers' data centers. If they go down for some reason there should be another back-up plan to ensure business continuity.

However, public-facing cloud-based services such as Facebook and LinkedIn are under constant attack as they hold the crown jewels from a criminals' perspective – data. Being on these sites can make good business sense but accounts also have to be well-managed to avoid data security lapses and employee use of the sites must also be monitored to ensure it doesn't end in business PCs being infected. Malicious links and other tricks abound to try and get you to download data stealing malware.

Security pros and cons of cloud computing

Pros

Data security standards are likely to be higher in your provider's environment than in your business, especially if the cloud provider is accredited with ISO and other key industry standards.

Your cloud provider is likely to be better resourced physically and financially, to cope with data security threats to its infrastructure than you.

Your data will still be available, even if you lose a laptop.

Cons

Your data will be stored outside the business network, and possibly even abroad, which may contravene local data protection laws and regulations.

If your internet connection is unstable there may be problems accessing your services.

Sites like Facebook and Twitter are highly prone to attack. A hacked corporate account could do more damage than good from a reputational standpoint, while careless use of the sites by an employee could give criminals a foothold inside the network and an opportunity to mine customer data.

Automatic data back-up and high levels of security are not guaranteed – due diligence must be undertaken.

How to be more secure in the cloud

Ensure you check into where your data is stored and what security measures are in place from your provider.

Think about a cloud-based secure back-up and online synchronization service for all your data which currently resides on-premise. Lost devices can be a major headache but are ultimately replaceable – your customers' data isn't.

Invest in security software which leverages a cloud-based threat protection network, preventing most email and web-borne malware threats before they even reach your desktop, laptop, mobile or network and allowing you to enjoy the benefits of cloud computing while minimizing the risks.

For mobile devices this combination of local client software with cloud protection means most of the workload can be dealt with in the cloud, freeing up the phone's processing power for other tasks.

Encrypt data wherever possible to minimize the risks associated with data loss.



On social networking sites, ensure your account is safe with strong password and different passwords for each account. Make sure staff are trained in safe browsing.

IT Security can be a difficult for a non-expert to keep on top of. One option would be to outsource management of this to a Value Added Reseller (VAR) or managed service provider who can be the de facto IT department for your business. Cloud services can then be used by this partner to manage all of your security.

Cloud computing, as we have seen, can be a wonderful business enabler. However it is for you as a small business owner to calculate if it's the right fit for your current environment. If the limited risks can be properly managed, though, it promises cheaper, faster and more efficient ways of working which could help your business achieve stellar performance

