INTRACLOUD
connecting business

Cyber attack, Ransomware, stolen laptop or just plain mistaken file delete – can you afford to remain unprotected?

7th. February 2017

A recent study has revealed that for a small business 60 minutes of downtime comes with a hefty cost of £5k to £8k. Even for a micro business the costs exceed £1k per hour and typical downtime due to hardware failure is between 14 and 96 hours. However, these are the lesser of two evils.

In this week's article we will be talking about the huge growth of cyber attacks targeted toward the small and micro business.

You can't seem to get through a day without a new story surfacing of another company's data breached, service denied, ransom demand or personal records stolen. Although it is generally the big names that make the headlines the real concentration of attacks are aimed at the other end where numbers are much larger, defences are much weaker (if at all) and payment is more likely to be made in a short space of time.

The FBI estimated last year that Ransomware payments in the United States were on pace to hit $1 billion, compared with $24m paid to cyber attackers in 2015. The U.S. government also estimated that Ransomware attacks averaged more than 4,000 per day in 2016, up from the approximately 1,000 attacks per day in 2015. The average demand was for $10,000 and most were aimed at small and medium business. It's not surprising that Ransomware is being forecast to the fastest growing industry in 2017.

Could it happen to you?

Industry analysts are advising all businesses to accept that it is not if but when. Indeed there are hundreds or even thousands of cyber attacks carried out every single day that will not be reported by the media – or, in most cases, the victim. It is estimated that any device connected to the Internet receives between 800-1200 automated attacks per minute from robots and not humans. So it is also a faceless, relentless activity that never sleeps.

INTRACLOUD
connecting business

What can you do to defend your business both night and day?

Nothing and paying the ransom if you are compromised is not really an option. The ransom asked is in the Internet currency of bit coins, which are not traceable. If you pay you are likely to experience one of the following; nothing bar the loss of the ransom money and your business still in lockdown, a demand for even more money and at best an encryption key that requires technical knowledge and considerable time to implement. Regardless your name will be sold on the dark web as a good target. At this point the ransom payment will be the tip of the iceberg when it comes to costs.

Just carrying out backups is also fallible and only really a reactive level of defence. If they are not automated and regularly tested they cannot be relied upon and the latest intrusions are also designed to stay hidden, whilst they become firmly embedded in the backup files. That way they have you and your backups held to ransom.

The best approach is to be proactive. Regular backup with continuous Malware threat detection together with fast system restore getting a business from disaster to business as usual in under an hour, is possible. It is also possible to backup not just the data but also the physical hardware (servers, laptops etc.) as images or 'bare metal backup', operating systems, applications, databases, drivers, active directory, cloud and SaaS (Office365, GoogleApps). In effect the whole IT infrastructure whether this be one laptop, a Server Room or a hybrid cloud model. So it's like having a virtual datacenter in the cloud, available to serve your business when necessary.

The data sovereignty can be specified to be solely within the United Kingdom with data being encrypted to AES256-bit both in transit and at rest. Granularity of data access can also be down to file level and all backups would go through a verification process that includes advanced Malware detection. If Malware detection is made it is immediately quarantined in a sand-box for safety. Certification to ISO27001, ISO9001, IL4, ISO27032, and ISO20000 are also the standard.

Whilst nothing can be absolutely 100% secure, following this process will cover you for 99.999% of all threats. That's the equivalent of a whole year except the last 9 seconds. So pretty secure and professional.

INTRACLOUD
connecting business

So, where do contractors fit in?

Contractors more than anyone understand that no work equals, no income. For many no laptop also means, no work.

The responsible contractor needs to protect himself and his business against this type of threat. To get full protection that also covers loss, physical theft, hardware failure, erroneous file deletion, ransomware, virus attacks and denial of service can be achieved for a very modest investment. For most the annual costs are less than a days pay and work out to less than £2/day for a single laptop with 500GB of data. It's a small price to pay for the security delivered and allows you to concentrate on your business and not the threat to your IT.

www.intracloud.co.uk infocloud@intracloud.co.uk