KCS Group Europe

Cloud Nein: The Dangers of Offsite Storage

04/12/2017

The world may be moving to *'the cloud'*: heralded as the ultimate repository for data and ease of access in the modern age. However as the latest leak from the Pentagon has showed, the cloud is just as susceptible to security flaws as other methods.

100GB of data was left on a public Amazon cloud server for at least four years, freely viewable by anyone who knew where to look – or who just happened to come across it. While this data came from a failed intelligence-sharing program, the trove it contained was gold dust: private keys, hashed passwords, intelligence gathering platforms, and a virtual transmission drive for sending and receiving data. If even one aspect of this load was in use today (and one suspects that passwords in particular may not have been changed), then there could be a severe compromise here.

What is worse, this comes from the Pentagon – one of the very organisations which should know better and safeguard even the most innocuous piece of information as if it is the nuclear codes.

This incident highlights the dangers inherent in cloud security. If online storage becomes the norm, then we risk losing total control over our own data – and what is done with it. Data stored on an internal system or a physical medium is a lot harder to compromise than data which is "out there" in the cloud – as indefinable a place as The Internet itself – for reasons of oversight and foreknowledge. Not only can the cloud be attacked through more vectors than an internal system, because it is likely to be shared my multiple customers, but because you do not actually own the storage box in which you are placing your possessions. This also puts you at risk from the service provider being hacked, or your data being 'sold on' through mailing lists which may themselves reach into the Dark Web.

The question comes down to the degree to which an organisation feels that control over its data is offset against the ease and 'fire-and-forget- nature of using a cloud system. In the short term, a cloud bay be useful but with a longer view it is almost always worth maintaining an in-house solution. Besides, security should be the overriding concern where public data is concerned. Not just the data held by the Pentagon, either.

It remains to be seen what impact the implementation of GDPR in April next year will have on whether, and how, companies use the Cloud. This (and any punishments that arise from a failure to take GDPR seriously) will once again re-ignite the debate over where the balance lies between organisational security and – perhaps - organisational efficiency. But for businesses using the Cloud at present, there

are standard security steps that can and should be taken to minimise the risk that the Cloud poses. Ensure that all credentials are up to date and changed regularly. Request that your Cloud provider can guarantee the security of all information uploaded, including with facilities to monitor for service abuse, DDoS attacks and any shared technology. Ensure that backups are still maintained in-house, physically if need be, to guard against catastrophic data loss. And conduct regular sweeps within the Dark Web to pick up on anything left lying around – something which could have saved the Pentagon a great deal of embarrassment.

Remember – clouds can burst, and nobody likes the rain!