Tape Encryption – Why you should consider it!

Backups are often an overlooked item when people are considering the security of the information on their systems but there are some things that must be considered when discussing any overall security needs on a system.

The reason that this often gets overlooked is that the people investigating the needs of security most often come from a networking environment, so would be looking at things like intrusion detection and prevention, multi factor authentication, access control and the many technologies that surround these requirements.

What they may fail to take into consideration is that all the data they are concerned about its most likely written to a high capacity backup tape on a daily basis and them removed from site in case it is needed for a system restore in the case of lack of access to the main system for whatever reason, flood, fire, building damage or actual system failure.

What needs to be considered is the fact that the backup is given access to all the data, this is done so that a full and complete backup of all the corporate or system data is taken, to ensure that if it is necessary to restore systems or corporate date, it has been backed up and is available to be restored. There is an audit to show what has been backed up but that is designed to allow checks to be made to ensure everything has been included, not to audit who has had access to the data. Once on the tape there is no further audit to see who reads it or when, unless this is done on the system it was saved on. Should someone take that tape to another system they can access it, copy it or even make changes to it without any of these changes becoming known to the system administrators.

It should be clear from this that any data that is being held on your systems and being backed up to tape or similar removable media devices can be compromised without any knowledge of this fact. With modern tape media being capable of recording over one terabyte on a single tape it can be seen that the amount of information that can be lost or compromised from a single tape is substantial.

With the alarming increase in reported data losses due to tapes being stolen more and more companies are now looking at ways to ensure any tape losses do not hurt their business or their customers. The main way to do this is with tape encryption. Once tape encryption has been implemented the system administrators can ensure that the data they backup to tape has been encrypted, this means if the data has been taken offsite the data's integrity will not be compromised.

There are several approaches to implementing tape encryption; one way is to encrypt the tape from within the backup programme. Once you start to look at this there are however a number of pitfalls and problems that come to light. The first being the fact that the existing backup package may not offer this option and then if it does it could be found that the pricing is based on the number of tape drives and tape media the package is supporting. If you have several tape drives or a vast number of tape media under the backup software, the pricing can start to become unexpectedly high.

The second issue that becomes apparent once this is implemented is the fact that the system now has an additional overhead when completing the backup, as it now has to encrypt the backup data as well as completing a full backup of the data. It maybe that the system has the spare processing power to handle this process without any impact on other jobs, however as the system is unlikely to be designed to handle the encryption of data, due to this it may put additional strain on the system. Then you need to consider the impact when doing a system restore as this may mean that you are unable to meet your service level agreements (SLAs), as you may also be unable to do a bare metal restore as you first have to setup your backup software so that you can decrypt the data held on the backup tape. One fact that will also impact the use of software is the fact that encrypted tape backup data cannot be compressed and that tape drives utilise data compression to get the higher transfer speeds and capacities. The way to overcome the problem this can cause is to compress the data prior to encrypting it, but if using the software on the system to do this it will add another processing overhead to the backup.

The solution to the many problems associated with software for tape encryption is to utilise a dedicated hardware tape encryption appliance to do the work, this means that you are using a specifically designed hardware appliance to encrypt your tapes.

This is where the Paranoia family of products fits, the Paranoia range of tape encryption appliances offer secure encryption via dedicated encryption engines, and also offers pre-compression of the data, this reduces the effects on the throughput, because the Paranoia's pre-compression engine is powerful there are circumstances where it may even increase the throughput of the tape, utilising a Paranoia tape encryption appliance overcomes the problems you may encounter using software encryption as they have been specifically designed to encrypt a tape. Another advantage of the Paranoia range of products is that you can do a bare metal restore from tape, as the Paranoia appliance is completely transparent to the system and the tape appliance.

The Paranoia unit fits between the tape drive and the system, encrypting the data '*on the fly*' and requires no changes to the operating system or backup software. This also means there is no need to upgrade your tape technology as it will work with all tape drives. Because it will work with all system types the Paranoia can be utilised across the complete company IT landscape so making support and DR simpler.

Silverstone Innovation Centre
Silverstone Circuit
Silverstone
Northants, NN12 8GX,
United Kingdom

Phone: 01327 856070
Fax: 01327 856071
E-mail: sales@disuk.com

DISUK
Tape Encryption