

## THE ENCRYPTION EVOLUTION

STRONG PROTECTION OF DATA AND EASY USER ACCESS ARE NOT MUTUALLY EXCLUSIVE SAYS ANDERS PETERSSON, CSO AT BLOCKMASTER

With data proliferating across organisations and mobile working increasing to maximise operational flexibility and efficiency, protecting information inside and outside the corporate boundary is one of the biggest headaches IT departments are facing today. This, coupled with the growing threat of systems being hacked into, insider attacks, and the vulnerability of removable media being lost or stolen, creates quite a challenge for IT departments.

It is alarming to observe what seems to be a lack of efficient security technology and processes in place to protect data, but this is - in some part at least - due to the constant battle between providing comprehensive protection and not impacting on user convenience and behaviour. The key to this is for organisations to invest in encryption, which can be centrally managed to provide peace-of-mind that data is always secure. This way, any data compromise shouldn't turn into a breach or worse still, irreversible brand damage or penalty.

To ensure that all stored data is secure, organisations must establish and implement a policy enforcing encryption across all storage media, including computers, servers and removable devices, such as USB sticks. The use of software to encrypt desktop hard drives is commonplace, but there are a huge amount of insecure USB drives being used to carry around valuable company information, which have no protection at all. As a standard, USB drives should have

military grade hardware encryption, which generates its key within an embedded system on the flash drive itself, and applies 100 per cent of the available encryption power, irrespective of the password length or complexity. This encryption is as strong as the algorithm, unlike software encryption, which is as weak as the user chosen password. Unprotected drives also come with a number of hidden security risks, including data being hidden when the user thinks it is deleted and data becoming corrupted by faulty flash components. Even software-encrypted files are at risk from parallel offline attacks with rainbow tables and software tampering applications.

An audit of all storage media must take place to assess which devices need protecting and by which type of encryption. To get the best of breed technology it is likely that several encryption vendors will be involved in securing information across an organisation. It is important that AES 256 encryption is set out as a standard requirement as it is the highest grade and most robust level of encryption that can be used. The encryption technology must be combined with effective management tools to ensure devices are easy-to-use and therefore willingly adopted by employees.

As with all technology purchases the IT team must test the products thoroughly in a range of scenarios to ensure their robustness and ease-of-use. Organisations must also test how they would recover data if an employee forgets their password or leaves suddenly, as well as the ability to

manipulate and delete data from one central location.

The next stage is roll-out and employee adoption. It is imperative that internal communication tools, such as newsletters, are used to publicise the encryption technology and its benefits, as well as communicate the consequences of not complying with the new security procedures. It is likely that some staff will not understand or see the value of encryption, so advising of policy development and implementation will ensure processes can be implemented with minimal disruption.

Increasing amounts of data should not be seen as a nightmare for organisations. As long as security is built in up front, and across all storage media, with a focus on the most robust encryption technology available, IT teams will be able to rest easy at night, knowing that company data is secure, but flexibility in accessing this data is not impaired. **CS**

