Why encryption is the best strategy

Data protection, wherever it resides, must form the core of companies' security systems, says **Colin Tankard**, managing director at Digital Pathways

SHUTTERSTOCK/MORROWIND

Encryption, in which information is converted from a readable format into one that obscures its meaning from those without the authorisation or ability to decipher it, has long been used to protect sensitive information from prying eyes.

Data security as a pressing concern

In recent years, ensuring the security, confidentiality and integrity of data has become an ever more pressing concern. Information and data produced and collected by organisations, including intellectual property and personally identifiable information related to customers, employees and business partners, is valuable not just to the organisation concerned, but also to criminals who can use it for financial gain.

According to recent research by Vormetric, 91 per cent of IT executives state that they feel vulnerable to data security threats; and with good reason since data breaches are everyday news and can impact any organisation, no matter its size or line of business. A recent government survey found that whilst 65 per cent of large firms reported having suffered a data breach in the past year, more than half of medium-sized firms and one-third of small organisations had been breached, showing that no one is immune. Gemalto has released a report that showed that businesses in the UK suffer the highest level of breaches in Europe, and are second only globally to the USA.

According to Breach Level Index, almost 5 billion data records have been lost or stolen since 2013, but only 4 per cent of those records were encrypted. Any data breach can cost the organisation that was involved dearly, both in terms of lost revenues and damage to its brand and reputation. The Department for Business, Innovation and Skills states that cyber security is a growing threat for all organisations, costing large businesses an average of £1.5 million, up from £600,000 in 2014, whilst the average cost for SMEs has doubled to £310,800.

The key role of encryption

Encryption has a key role to play in keeping sensitive and confidential information safe from criminals and prying eyes. The use of encryption is the best strategy for any organisation for maintaining security for any information when it is in storage or is being transmitted, such as over email. Originally considered to be a complex technology to deploy and manage, the technology has moved on and can now be easily used by anyone.

But it is not just a good strategy to choose to encrypt sensitive data, it may also be required. Organisations face a wide range of regulations and industry standards that they must adhere to and that are increasingly strict with regard to protecting sensitive data. In the USA, the majority of states have laws regarding data breach notification and those doing business in Europe will face similar pressures when the General Data Protection Regulation (GDPR) becomes law in May 2018. As with most directives and regulations produced by the EU, the GDPR is not particularly prescriptive in terms of technology to be used, with the exception of encryption and pseudonymisation, which are specifically 'called out' as suitable, appropriate safeguards for protecting data.

A safe harbour where encryption is used

What many of these regulations and industry standards such as PCI-DSS for protecting payment card information have in common, is that they provide a safe harbour when encryption has been implemented. For example, the majority of laws that mandate data breach notification contain clauses whereby notification is not required where data that has been lost or stolen has been encrypted, since the data cannot be compromised unless the encryption code or method is also compromised.

Encryption in overall security strategy

Encryption by itself is not the only technology that organisations should have in place to protect sensitive data, but should be a strategic part of the entire security system, alongside complementary technologies such as access controls, monitoring systems, and auditing and reporting capabilities.

Of particular importance is that the actions of privileged users are tightly controlled in terms of what they can access and what they do with information. This is necessary owing to the need to counter insider threats, which are estimated to account for 43 per cent of all breaches, many of which are attributed to actions by privileged users. Not all insider threats are caused by malicious intentions, as accidents can occur such as inadvertently sending information to a recipient other than that which was intended; but insider threats can be the most damaging since internal users can have access to the most sensitive and valuable information that an organisation possesses. These controls should be tightly integrated so that there are no security gaps that could be exploited so that organisations are better able to both 'ward off' advanced threats and meet their compliance objectives.

Encryption should be applied across all areas, devices and cloud services. The latter can be achieved with the use of a cloud encryption gateway that provides robust, persistent controls, detailed visibility regarding data access and the ability to detect unencrypted files. Such technology not only ensures that risks are reduced, but also provides full auditability so that compliance requirements can be met and proven.

Another core capability is cryptographic key management, which should be centralised to ensure that policies can be consistently applied across all data, both when in transit and when at rest. Efficient key management can be achieved through use of a physical or virtual appliance or, increasingly can be provided as a service, especially for cloud applications.

Encryption as a baseline

The importance of having such controls in place to protect sensitive data is only set to grow. Organisations that have not yet started preparing for compliance with the GDPR should be looking to do so now as there is only just over a year to go before compliance is mandatory. In comparison to previous data protection laws it is considerably more stringent and impacts a wider range of organisations than before.

Encryption should be considered to be a core part of any data security strategy that organisations develop, both for data at rest and in motion. For both data security needs and for achieving regulatory compliance, encryption should be considered to be a baseline.