WINTER 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their e-discovery, computer forensics and cybersecurity needs. With increasing encryption usage and the recent news of the government requesting Apple to provide "backdoor" access to iPhones, we chose to theme this E-Newsletter on the impact data encryption has on attorneys, litigation support professionals and investigators.

KEEPING THE KEYS TO THE DATA KINGDOM SAFE

In the face of both internal and external threats to an organization's electronic data, many organizations look to encryption as an effective safeguard. For organizations that employ encryption as part of their data security operations, encryption keys are as vital as the combination to the corporate safe, the recipe for the secret sauce, or the code for the next release, all of which may well be protected by encryption. Controlling the use of encryption by managing encryption keys is a critical part of data security. Prior to implementing an encryption key management practice, an organization must address essential questions or risk compounding an already complex issue. We will explore these questions and possible answers along with possible future topics in this article.

The complexity of managing encryption keys multiplies exponentially as, among other aspects, an organization increases the amount of data encrypted, the types of encryption utilized, and the number of key holders within the organization. Despite best practices, employee key holders may unintentionally be the weakest link within the e-security cycle. Inevitably, people within any given organization will lose their encryption keys, staff changeover will occur, and IT departments will be recruited to spend valuable time retrieving keys. Despite the potential headaches that may arise from within an organization, external threats may be an even greater reason to practice encryption key management.

Unfortunately, not all encryption technology is used for good. Ransomware attacks have been on the rise as of late. Ransomware spreads much like a virus when a user downloads malware via an executable file, infected email, or visits a spoofed website that uploads the malware onto the victim's computer. The ransomware then encrypts certain files such as Office (.docx, .xlsx, pptx) or PDF files. When the victim tries to open the file, a ransom note appears instead, telling the victim to pay a ransom, most often in Bitcoin (BTC) to obtain the key to decrypt their files. In some cases, infection isn't limited to one computer, but spreads throughout an entire network including file shares, email servers, and other critical systems. Performing daily backups and having a robust disaster recovery plan in place can certainly help mitigate some of the harm of such attacks.

The first question that an organization needs to consider is whether central control of encryption keys is warranted and/or desired. An organization with a decentralized infrastructure operating in disparate locations may wish to increase flexibility and responsiveness through multiple points of control. Once that determination is made, the twin questions of who will control the process and where that control will reside need to be addressed. In a 2015 global survey on e-security*, 58% of respondents indicated that *who* and *where* questions of control were the most difficult aspects of implementing an encryption key management practice. For the purposes of this article, we will assign the role of key management to IT departments, a practice which coincides with the predominant trend.

Once the if, who, and where of encryption key management is settled, an organization can address how the encryption keys will be generated, changed, and destroyed. Allowing individual keyholders to self-generate keys using software such as Veracrypt or Diskcryptor, creates the almost impossible task of tracking these keys. Without an audit trail to aid in key generation, let alone tracking the details of such as encryption key expiration dates, IT department response to key loss or staff change is limited.

Additionally, how these encryption keys are stored and protected is of paramount importance. Again, if individuals are allowed to generate keys themselves, and these keys are subsequently stored in plain-text files and/or sent in email, they lose their protection. If, for example, a user uploads encrypted data onto an online file sharing platform such as Dropbox or Box.net, then leaves the organization without transferring the key to his or her successor or without maintaining an accessible record of the key, the data is potentially rendered forever unusable, even if it was downloaded from the online file sharing platform.

Best practices suggest that encryption keys need to be stored in a secure repository where designated staff can monitor, regulate, and protect encryption keys. Typically, these keys would be stored on hardware that is located separately from where the encrypted data is stored. One additional issue that may arise in relation to key management is backward compatibility with different versions of the same encryption software. Maintaining accessibility to the same version or a newer version of software to decrypt data when necessary is a prudent undertaking to ensure future availability of older data.

Numerous key management systems (KMS) that are both proprietary (e.g. IBM, HP, Vormetric) and open source (e.g. Vault) are available to facilitate the process. These KMS software solutions offer flexible, scalable, and secure unification of key management accessible through direct connection via server or through a web interface. KMS can also provide an administrative master key, which acts as a recovery key for all of the other keys stored within the KMS. The master key needs to be protected as vigilantly as a bank vault with proper credentials and redundancy in key staff.

The complexity of managing encryption keys across an organization isn't likely to diminish anytime soon. As data comes under attack from security threats both external and internal in nature, an organization is well advised to consider carefully how encryption will be used and effectively managed. Just as consumers are warned to guard their personal information judiciously, organizations need to implement viable solutions for daily operations, and continuous employee education to prevent data loss and/or theft. Finally, having a partner, such as Digital Mountain, ready for incident response becomes a necessary means to ensure that the keys to your data kingdom are safe and secure.

*Thales 2015 Global Report on Encryption and Key Management

UPCOMING INDUSTRY EVENTS

February-March 2016

RSA Conference, San Francisco: February 29 - March 4

March 2016
Fifth Annual ASU-Arkfeld
eDiscovery and Digital Evidence Conference, Tempe: March 9-11

ABA Techshow 2016 Conference and Expo, Chicago: March 17-19

April 2016
The Masters Conference, San Francisco: April 19

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT:

in f 🐦