Respecting data privacy rights through data encryption

Data rights are human rights. Whilst that principle is embedded within and encouraged by data regulations, including GDPR, DPA, CCPA and HIPAA, it is counteractively provoked by technologies, such as live facial recognition surveillance, that carry the looming risk of abuse and weaponization. Data privacy is often the price for services, whether it be police protection, app use or be given targeted, more relevant advertisements. This dichotomy has been the source of much debate, scrutiny and concern.

Data privacy must be a top priority for all organisations and should be considered from the outset of data sharing initiatives. Of course, avoiding hefty fines, job losses or suffering brand damage are all significant impetuses to protecting data. However, respect for consumers' data privacy rights will drive organisations to go the extra mile to ensure data confidentiality.

This begs the question; how can data privacy be achieved? Whether or not data privacy, on a wider and global scale, can ever be truly achieved would perhaps be a more appropriate question. However, small measures taken to keep sensitive information protected and confidential can have a positive ripple effect. Individual organisations can take the lead in respecting their customers' data privacy by encrypting data in transit and at rest.

How can you encrypt data in the cloud?

Encrypting data is a requirement of most compliance standards. Yet, a recent study found that an alarming 43% of cloud databases are not encrypted. Organisations are under constant attack and, regardless of whether the attack makes headlines or not, the data should be protected. To ensure data privacy when faced with common threats, such as DDoS and malware attacks, data must be encrypted before it is sent to the cloud, in transit and at rest.

For ultra-secure encryption, that data should preferably be encrypted with a FIPS certified randomly generated AES 256-bit encrypted encryption key. Confidential information stored on a local computer or drive, sent via email or file sharing services (such as WeTransfer) and shared in the cloud should be securely encrypted.

The more people the data is shared with, the greater the challenge to ensure data privacy. Storing data in one place and accessed by authorised users only, who have a copy of the encrypted encryption key at hand, can allow for efficient working whilst ensuring data security. Sharing encrypted data securely allows for instant collaboration in the cloud, saving time in what would be days of posting encrypted USB flash drives to and from colleagues.

> "Data privacy must be a top priority for all organisations"

Controlling the encryption key

If the data is stored in the cloud, control of the encryption key is important. Granted, most cloud service providers (CSPs) will encrypt their customers' data and some even offer a key management system service, which allows customers to manage their encryption keys. However, the encryption key is stored in the cloud and thus accessible to hackers and cloud staff – much like leaving your house key under the doormat that half the neighbourhood knows about.

The user needs full and secure control of the encryption key in order to ensure the data is kept confidential even if the cloud account is hacked. Having your own key management system will not only give you more control of encryption keys but is also more convenient for those using a multi-cloud solution.

Security measures must go beyond the cloud login credentials. If a hacker obtains the user's credentials, the breach will go unnoticed to the CSP as they won't be able to decipher between a legitimate user from an attacker. By keeping the encryption key, which should be encrypted itself within an ultra-secure Common Criteria EAL4+ ready secure microprocessor along with a PIN authenticated code, away from the cloud increases the number of security measures from just one authentication, the cloud account login, to as much as a five-factor authentication.

Back up encrypted data using USB flash and hard-disk drives

Backing up valuable data onto an encrypted hard-disk drive can save organisations the trouble of losing access to important information during a ransomware attack. Using a PIN protected hard-disk drive will secure the data even if the drive is lost or stolen, avoiding the risk of their data being accessed or viewed by unauthorised persons.

To avoid losing sensitive information in the event of a ransomware attack, sharing information using PIN protected USB flash drives is another safe option. This can be especially useful for remote workers as they can securely protect and back up their confidential data whilst on the go.

Encrypting data within a unique and dedicated hardware based Common Criteria EAL4+ ready secure microprocessor is the ideal solution. The ultra-secure microprocessor employs built-in physical protection mechanisms, designed to thwart cyber-attacks, such as side-channel attacks designed to defend against external tampering, bypass laser attacks and fault injections.

All critical components within the drive should be covered by a layer of super tough epoxy resin, which is virtually impossible to remove without causing permanent damage to the critical components. If breached, the drive's tamper evident design will provide visible evidence that tampering has occurred.

Brute force limitation is an excellent feature to look for in a drive. If the PIN is entered incorrectly 10 consecutive times, the PIN will be deleted and the drive can only be accessed by entering the Admin PIN to reset the User PIN. If the Admin PIN is entered incorrectly 10 consecutive times, the encrypted encryption key is deleted along with all data previously stored in the drive.

Conclusion

To keep sensitive information confidential, data stored locally on a computer, on a drive or in the cloud, or shared via email or file sharing service, must be encrypted. Data encryption is an important stride towards data privacy, helping organisations comply with regulations like GDPR. As fears of a looming Big Brother dystopian future grow and as data breaches hit headlines on a regular basis, organisations can stand out as data privacy pioneers and earn their customers' trust.

> "The user needs full and secure control of the encryption key in order to ensure the data is kept confidential"

iStorage is the trusted global leader of award-winning, PIN authenticated, hardware encrypted portable data storage & cloud encryption devices. iStorage offers the most innovative range of products to securely encrypt, store and protect data to military standards; safeguarding valuable and sensitive data to ensure compliance with stringent regulations and directives such as GDPR, HIPAA, SOX, NRC, GLB and DHS Initiatives. Today, iStorage products are used by government, military, multinational corporations as well as consumers in over 50 countries, with the mantra that encryption is an essential commodity required by all.