KASPERSKY lab

BEST PRACTICES

Encryption

www.kaspersky.com

YOUR GUIDE TO ENCRYPTION BEST PRACTICES.

Data Protection. Act.

Proactive data protection is a global business imperative. Kaspersky Lab can help you implement many of the best practices around data encryption and protection.

The Business Case for Encryption

More than **816** million records have been compromised since 2005.[1] In the first four months of 2015 alone, over **101** million records were exposed.[2]

Hardly a week goes by without news of a major data breach hitting the headlines. The Identity Theft Resource Center, naming 2014 'The Year of the Data Breach,' flagged data stored on mobile or removable devices, along with internal breaches caused by unauthorized employee access to sensitive data, as two of the leading causes of data loss or leakage.[3] Almost one in five companies surveyed by Kaspersky Lab have suffered data loss as a direct result of device theft.[4]

Kaspersky Lab research has found that the average cost of a data loss incident in 2014 was **$636,000** for an enterprise and **$33,000** for a Small-to-Medium Business.[5] And you don't have to physically lose a device to lose sensitive data. Sensitive business information, intellectual property and trade secrets have become core targets of malware attacks.

It's not just about the direct cost of a breach, loss of loyal customers or damage to your company's reputation (72 per cent of companies have had to publicly acknowledge an incident[6]), in most major markets, data security and privacy are now mandated by law, with many jurisdictions obliging organizations to encrypt sensitive data.

From PCI-DSS,HIPAA, SOX, EU wide DPP, Japan's PIPA or the UK's DataProtection Act, the global trend is towards authorities requiring that companies proactively protect sensitive data. In the UK, for example, the Information Commissioner (ICO) has said that data losses occurring "where encryption has not been used to protect the data" are likely to result in regulatory action.

Whether you're faced with a stolen laptop, lost storage device or data stealing malware, encryption means your sensitive data is useless to criminals or unauthorized viewers.

So what's the best way to go about it?

[1] Privacy Rights Clearing House: http://www.privacyrights.org/data-breach
[2] Identity Theft Resource Center 2015: http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReport2015.pdf
[3] Identity Theft Resource Center 2015: http://www.idtheftcenter.org/Press-Releases/2014breachstatistics.ht
[4] Kaspersky Lab: 2014 IT Security Risks Report
[5] Kaspersky Lab: 2014 IT Security Risks Report
[6] Kaspersky Lab: 2014 IT Security Risks Report

Best Practice Approaches to Encryption

Kaspersky Lab's encryption technology protects valuable data from accidental loss, device theft and targeted malware attacks.

1. POLICY FIRST, TECHNOLOGY SECOND

As with so many security strategies, best practice for encryption begins with establishing strong policies: Are you going to encrypt entire disk drives? Removable storage devices? Or just certain kinds of data, files and folders? Maybe you want certain documents to be unreadable to some users but not to others? How about a little bit of both?

For most businesses, making information accessible to the right people at the right time is a priority – good policies, coupled with the right technologies will get you there without compromising on security.

Some good places to start include:

- **Involve all relevant stakeholders** – IT management, operations, finance, HR etc. They'll help you to identify the kinds of information that need extra protection.
- **Access control** – If everyone's got a key, there's no point in locking the door. Work with stakeholders to identify who needs access to what kind of information. And when. As an extra precaution, audit access controls regularly to keep them relevant.
- **Know your compliance needs** – PCI-DSS, HIPAA, SOX, EU wide DPP, Japan's PIPA or the UK's Data Protection Act. You might not be familiar with the growing number of data protection regulations out there, but many of your co-workers are. Identify the regulations, laws, guidelines and other external factors that govern the way data is secured or exchanged in the organisation. Set policies to work with these – for example automatic encryption of customer credit card data or employee social security numbers.
- **All in or all out** – Put your policy in writing, have senior management endorse it and communicate it to your end users – including any third parties that handle your sensitive data. If they don't like it, that's fine – but they can't have access to your data.
- **Back it up** – best practice always involves backing up your data before installing any new software. Encryption is no different – make sure you back up all your end-user's data before proceeding with your encryption programme.
- **Keep it simple** – minimize end user burden and intrusiveness by implementing technology that supports single-sign on.

2. FULL DISK ENCRYPTION OR FILE LEVEL ENCRYPTION?

The simple answer is: Both.

Encryption solutions typically come in two key varieties – Full Disk Encryption (FDE) and File Level Encryption (FLE), each of which has its own set of benefits:

Benefits of Full Disk Encryption (FDE):

FDE is one of the most effective ways any organization can protects its data from theft or loss. Regardless of what happens to the device, FDE allows organizations to ensure all sensitive data is completely unreadable and useless to criminals or prying eyes.

- FDE protects “data at rest” at a level as close to the hardware as possible – i.e. every single sector of the drive is encrypted. The means that all the data on your hard drive is encrypted, including file content, metadata, file system information and directories structure. Only authenticated users can access data on the encrypted drive. In addition to hard drives, FDE technology can be applied to removable media, such as USB drives or hard drives in a USB enclosure.
- Look for pre-boot authentication (PBA) – this requires users to present and authenticate their credentials before the operating system even boots, adding an extra layer of security. Nothing can be read directly from the hard drive’s surface by thieves, nor can the OS be started.

  Kaspersky Lab’s encryption technology provides PBA with optional single sign-on and also works with non-QWERTY keyboard layouts for better user experience. Encryption solutions that support smartcard and token authentication using Two Factor Authentication eliminate the need for additional passwords, improving user experience.
- Look for an encryption solution that features compatibility checks with all network hardware **before** implementation, saving headaches later. Solutions that offer support for UEFI-based platforms, including the latest laptops and workstations from Windows 8 onwards will ensure you’re future-proofed.

  Similarly, support for Intel AES NI – a new improvement to the Advanced Encryption Standard (AES) that accelerates encryption for Intel’s Xeon and Core processor families (as well as some AMD) – and the latest GPT disk standards contribute to a well-rounded encryption strategy.
- Enable secure data sharing within the business by using FDE encryption on removable drives.

- Best practice for FDE also includes a 'set and forget' policy, removing end-user choice from the equation; make access via a single sign-on (SSO) and your end users will be none the wiser. Two-factor authentication ensures an additional layer of protection and eliminates the need for additional user names and passwords, facilitating further ease of use. Encryption solutions that support Role Based Access Control (RBAC) enable the delegation of encryption management on a role/functional basis, for less complex encryption management.

FDE's greatest advantage is that it eliminates user error as a point of risk – it simply encrypts everything. On the down side, it cannot protect data in transit, including information shared between devices. If you're following best practice, and have chosen a solution that also offers File Level Encryption, this won't be a problem for you.

Benefits of File Level Encryption (FLE):

Operating at the file system level, FLE not only enables 'data at rest' protection, but also secures 'data in use.' Using FLE, specific files and folders on any given device can be encrypted. Best-in-class solutions allow encrypted files to remain encrypted, even when copied through the network. This makes selected information unreadable to unauthorized viewers, regardless of where it's stored or copied to. FLE allows administrators to automatically encrypt files based on attributes such as location (e.g. all files in My Documents folder), file type (e.g. all text files, all Excel spreadsheets etc) or the name of the application that writes the file – for example, a best-in-class solution will support the encryption of data written by, say, Microsoft Word, independently of the folder or disk.

- FLE offers great flexibility to businesses seeking to apply granular information access policies - only data defined as sensitive (according to administrator-set policies) is encrypted, supporting mixed data usage scenarios.

- FLE also facilitates easy and secure systems maintenance – encrypted file data can remain secure while software or systems files are open to facilitate updates or other maintenance. For example, if you're a CFO who wants to keep confidential business information out of sight of a systems administrator, FLE supports this.

- FLE supports effective application privilege control, allowing administrators to set clear encryption rules for specific applications and usage scenarios. Through application privilege control, administrators decide when to provide encrypted data in its encrypted form, or even completely block access to encrypted data for specified applications, for example:

    - Simplify secure backups by ensuring encrypted data remains encrypted during transfer, storage and restoration, regardless of the policy settings at the endpoint to which the data is restored.

    - Prevent exchange of encrypted files over IM without restricting legitimate message exchange.

By adopting a combined FDE/FLE approach to encryption, businesses can take a best-of-both-worlds approach – you might, for example, choose file encryption only for desktop PCs, while enforcing full disk encryption on all laptops.

3. ENFORCE REMOVABLE MEDIA ENCRYPTION

USB flash drives can now hold 100GB+ of data, while portable drives smaller than your hand can hold terabytes of data – that's a lot of potentially business-critical information being left in jacket pockets at the dry cleaners, left behind in the security tray at the airport or simply falling out of your pocket.

You can't control user carelessness or accidents, but you can control the consequences.

Effective encryption strategies include device encryption as standard. Ensure that every time sensitive data is transferred from an endpoint to a removable device, it is encrypted. You can do this by applying FDE or FLE policies to all devices, thereby ensuring that even when they are lost or stolen, your sensitive data is secure.

The most effective encryption solutions integrate with extended device control capabilities, to support the granular application of policies all the way to specific device serial numbers.

When working with sensitive information both inside and outside the perimeter, so-called 'portable mode' should be adopted. For example, you're making a presentation at a conference and have to use a flash drive to transfer your data to a public computer that doesn't have encryption software installed. You need to ensure that your data remains secure, even while it's travelling from your laptop to the presentation system – best-in-class solutions offer 'portable mode', allowing you to do this. It enables transparent use and transfer of data on encrypted removable media, even on computers where encryption software is not installed.

Choose Industry Proven Secure Cryptography

Your encryption strategy is only as good as the technology that underlies it. Easily cracked encryption algorithms are worthless. Choose an encryption solution that uses Advanced Encryption Standard (AES) with 256 bit key length with simplified key management and escrow. Support for Intel® AES-NI technology, UEFI and GPT platforms will future-proof your strategy.

Don't underestimate the importance of keys – your encryption algorithm is only as good as the key needed to unlock it. Easily hacked keys make your entire encryption program worthless. Similarly, effective key management is a vital component of effective encryption – there's no point in having the world's best lock on the door if you put the key under the mat.

Choose Multi-layer Security

End users and lost devices aren't the only causes of data loss. Data thieves are developing increasingly sophisticated malware capable of accessing systems and quietly stealing data, often going undetected for years. While encryption can help render any stolen data useless, it's much more effective when viewed as a complementary layer of a broader, integrated security strategy that includes high quality anti-malware, device and application controls that work together to reduce the opportunities criminals have to access systems and steal sensitive data.

No encryption best practice strategy is complete without integrated layers of anti-malware and controls-based protection capable of detecting and mitigating malicious code while scanning for, detecting and managing the kinds of vulnerabilities that expose organizations to data loss. All of this should be done with minimal end-user interference or even awareness.

Forgot Your Password?

Users forget their passwords almost as often as they lose their USB keys or smartphones.

Sometimes even the best hardware or operating system can fail, leaving users without access to vital information. Keep encryption keys in a centralized storage location/ escrow – this makes it a lot easier for you to decrypt data in emergency situations.

A quality encryption solution should provide administrators with tools for straightforward data recovery in the following cases:

- When the end user requires it (e.g. forgotten password)
- When the administrator needs it for maintenance, or in case of a technical issue, such as an OS that won't load or a hard drive has physical damage that must be repaired.

When a user forgets their password, alternative authentication can be achieved by requiring them to give the correct response to a series of alternative questions.

Manage Centrally

Encryption has acquired a reputation for being too complex to implement and manage. That's largely because more traditional, dated solutions are provided separately from anti-malware and other IT security technologies, generating unnecessary complexity. Managing diverse solutions – endpoint controls, anti-malware and encryption – even from a single vendor is not only expensive, it's time-consuming at all phases of the implementation cycle: purchasing, staff education, provisioning, policy management, maintenance and upgrade all need to be treated as separate projects for each component.

A fully integrated, multi-layer security solution not only saves time and money, but makes the software adoption process as easy and painless as possible.

Easy to manage solutions are more effective. Choose one that enables single console, single policy management from day one, reducing investment and eliminating compatibility issues between numerous components, all being managed separately.

It's good practice to apply endpoint encryption settings under the same policy as anti-malware protection, device control and all other endpoint security settings. This enables the best practice approach of integrated, coherent policies – for example, IT can not only allow approved removable media to connect to a laptop, but can also enforce encryption policies to the device. A closely integrated technology platform has the added benefit of improving overall system performance.

FINALLY...

Kaspersky Endpoint Security for Business can help make encryption best practice a reality for organizations of all sizes.

Complete integration with Kaspersky Lab's best-in-class anti-malware, endpoint controls and management technologies delivers true multi-layer security built on a common code base. This enables the application of encryption settings under the same policy as anti-malware, device control and other endpoint security elements. No need to deploy and manage separate solutions. Network hardware compatibility is automatically checked before encryption is deployed; support for UEFI and GPT platforms is standard.

This ground-up approach is possible because of Kaspersky Lab's unified code base – our developers create software and technologies that interact seamlessly, giving users an integrated security platform rather than a disjointed suite.

One vendor, one cost, one installation, complete security.

Twitter.com/
Kaspersky

Facebook.com/
Kaspersky

Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab