Information Security Updates

Data Encryption

Issue 7

Recent Incident

United Christian Hospital loses another USB drive

United Christian Hospital lost its second USB thumb drive in less than a month's time.
On 11 April 2009, a doctor, who is a resident in the obstetrics and gynaecology department, found her USB flash drive containing data of eight patients went missing. The data include patients' names and Hong Kong ID numbers, fetal heart scans, and a Powerpoint file that contains names and details of seven patients. In addition, neither data encryption or password protection was employed.
(http://www.alertboot.com/blog/blogs/endpoint_security/archive/2009/04/14/full-disk-encryption-on-usb-memory-sticks-missing-hk-hospital-loses-patient-records.aspx)

Related Article

Yale Laptop Theft Exposes 1,000 Health Records

Yale School of Medicine notified about 1,000 people whose clinical health information was contained on a laptop computer that was recently stolen from the school. While access to the stolen laptop was protected by a password, the laptop wasn't encrypted. The dean of the school of medicine apologized for the security breach and introduced several security upgrades, including mandated HIPAA security training, compliance with strong password standards, and "whole disk encryption," among others.
(http://campustechnology.com/articles/2010/09/03/yale-laptop-theft-exposes-1000-health-records.aspx?sc_lang=en)

I. Background

Industry Story

Desktop Encryption Project – University of Wisconsin-Madison

Laptops, desktops and other portable media that store restricted data are of great concern since they can be easily lost or stolen due to the distributed nature of their physical location and system administration. The purpose of desktop encryption is to render data on desktops and laptops unreadable so that risk is reduced if a computer storing restricted data is lost, stolen, compromised or disposed of improperly.

To mitigate or reduce the risks, the campus has approached the security vendor and implemented the following data encryption mechanisms:

- Full disk encryption for most flavors of Windows
- File and folder encryption for same flavors of Windows
- Full disk or file/folder encryption for Windows Mobile devices
- Centrally managed configuration and escrow of encryption keys

The Office of Campus Information Security (OCIS) has purchased 2000 licenses for campus use. These licenses are available to anyone wishing to participate in the project at no cost.

See this article:
(http://www.cio.wisc.edu/security/initiatives/encryption.aspx)

Data Encryption

With the growing amount of confidential information stored on end user devices, there are many threats causing such confidential information to be accessed by unauthorised parties. Some threats are unintentional, such as device loss or theft, while others are intentional, for example, malware threats, also known as malicious codes.

Data encryption leverages mathematical calculations and algorithmic schemes that transfer plain text into cipher text, a non-readable to unauthorised parties. As data encryption implant security controls inside sensitive data itself, it is now one of the most effective means to prevent leakage of sensitive information over transmission via the Internet.

Reference:
http://www.infosec.gov.hk/english/computer/encrypt.html
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

II. Management

Data Encryption Management

Data encryption can be either locally or centrally managed. Centralised management is more commonly deployed and performed through specific data encryption management utilities or together with the operating system's configuration utilities. Centralised management is recommended for most cases, because it enables effective and efficient encryption task management.

However, management may still choose to deploy storage encryption locally without a centralised management capability. This is generally acceptable for standalone or very small-scale deployments, especially for data that need to be encrypted quickly.

Data Encryption Planning and Implementation

A successful deployment of new encryption technologies very much relies on a step-by-step planning and implementation process which minimises unforeseen issues and helps to identify potential pitfalls. The following are the major task during planning and implementation phase:

1. Identify Requirements

In the beginning of the process, management should identify the needs to encrypt information on universities' information systems and/or end user devices, determine which device or data needs encryption, and define related performance requirements. The requirements include:

- **External Requirements** – such as legal requirement to protect privacy and personal data;
- **System and Network Environment** – data encryption solutions should be compatible with universities' existing IT environment (in terms of availability and efficiency) and able to provide the necessary protections without introducing conflicts and inefficiencies; and
- **Support Limitations** – identify any possible violations to the terms of a software support contract or the warranty of products used with the relevant device.

2. Design a Solution

Based on the requirements identified in the previous phase, management should design a solution to realise the requirements. Major aspects of a solution design of data encryption include:

- **Cryptography** – encryption schemes and algorithms, such as Advanced Encryption Standard (AES), Secure Sockets Layer (SSL);
- **Authentication** – authentication methods and authenticator protection. For example, passphrase, security token, public/private keys;
- **Solution Architecture** – selection of data encryption devices and software and location of centralised data encryption management;
- **Other Security Controls** – additional controls that complement the data encryption implementation, such as policies regarding acceptable use of data encryption technologies; and

Related Article

Liberty U Boosts Online Transaction Security

Liberty University in Lynchburg, VA has implemented a digital certificate management service from Verizon Business. The goal is to protect student information, financial records, and other confidential data. Designed for a university environment, the service provides a secure socket layer (SSL) certificate to Web site visitors during specific transactions to confirm to the user that the Web page is authenticated. It also encrypts the data--for example, credit card or social security numbers--passing between the user and the site. (http://campustechnology.com/articles/2010/05/19/liberty-u-boosts-online-transaction-security.aspx?sc_lang=en)

Related Article

A Buyer's Guide to Enterprise Data Encryption

You ask vendors if they can protect all your data, and they say yes. They tell you to trust that their "full", "complete" or "comprehensive" product will make all your data secure for years to come. What they don't tell you is that their product only protects "all the data" contained on specific devices, such as laptops, USB flash drives, or PDAs, That is a good first step, but how are you going to protect the rest of your data?
The reality of point products is: you will have to find another vendor to secure the rest of your data.
(http://download.pgp.com/pdfs/whitepapers/9Questions_061108.pdf)

Reference:
http://www.infosec.gov.hk/english/computer/encrypt.html
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

II. Management (cont’d)

- **Minimum Requirements of Hardware** – selection of hardware, including application servers, storage equipment and end user devices based on the requirements from product vendor and university's performance requirements.

3. Test a Prototype

It is recommended to perform implementation testing in laboratories or on test devices. The following components of the solution should be tested and evaluated:

- **Addressing Requirements** -- Each type of sensitive or critical data identified according to the information gathered during stage 1 should be protected with appropriate encryption methods;
- **Encryption Management** -- Robust testing of authentication should be performed, especially for centralised authentication solutions. Also, administrators should be able to configure and manage all components of the solution effectively and securely;
- **Performance and Compatibility** -- The solution should be able to provide adequate performance during normal and peak usage. Management should also ensure that the solution does not affect or interfere the use of existing operating system configurations and software applications;
- **Recovery** -- The solution should be tested to determine how well it can recover from failures, such as loss of encryption keys, damaged device hardware or software, and power loss; and
- **Implementation Security** – Vulnerabilities and weakness of storage encryption itself should be investigated and corresponding mitigation controls should be developed and tested.

4. Solution Deployment and Monitoring

Gradual migration of the new solution enables administrators to evaluate the impact of the solution and resolve issues prior to the deployment to the whole university.

Monitoring is essential to the successful deployment of a data encryption solution. It is to manage the solution by operating the deployed solution and maintaining the security storage architecture, policies, software and other solution components. Typical activities include:

- Testing and applying patches to storage encryption software;
- Monitoring the storage encryption components for operational and security issues;
- Periodically performing testing to verify that storage encryption is functioning properly;
- Performing regular vulnerability assessments; and
- Receiving notifications from vendors of security problems with storage encryption components, and responding accordingly.

Reference:
http://www.infosec.gov.hk/english/computer/encrypt.html
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

Related Article

Researcher eyes holes in Triple Zero radio

Emergency services are using weak and outdated encryption to secure digital radio communications, according to National ICT Australia researcher Steven Glass. Most emergency services use the 56-bit Data Encryption Standard (DES), which has been surpassed by much stronger levels of encryption and is considered unsafe, Glass told ZDNet Australia. Glass is conducting a PhD on emergency systems at Griffith University and is investigating the security of existing and future communications platforms. He also works in NICTA's Queensland research lab on the Safe II Networks project, which is working to mitigate shortcomings as well as improve performance and reliability in emergency networks. (http://www.zdnet.com.au/researcher-eyes-holes-in-triple-zero-radio-339307115.htm)

Related Article

New browser security tool may mean safer surfing

A Web security mechanism called HTTP Strict Transport Security (HSTS) is making its way through the IETF (Internet Engineering Task Force) standards process, and two of the major browsers are supporting it. Web sites that implement HSTS will prompt the browser to always connect to a secure version of the site, using "https," without the Web surfer having to remember to type that in the URL bar. (http://www.zdnet.com/news/new-browser-security-tool-may-mean-safer-surfing/483979)

III. General Users

Roles and Responsibilities of a General User

1. User Awareness

General users should comply with the data encryption policies set up by the management and be aware of their roles and responsibilities when they come to sensitive data stored in their device or in the campus network.

2. Encrypting Sensitive Files

Users should encrypt sensitive data according to the university's policy. They can make use of data encryption software when they need to send sensitive files over unknown or insecure network. Strong passwords, created in line with the security policy, should be used for encryption when files are being transferred into removable media or through email. Users must not record the passwords in plain text or release to unauthorised parties.

3. Portable Media Protection

Data encryption also has vulnerabilities that hackers may decrypt the encrypted data using advanced techniques or simply via social engineering. While encrypted removable storage device provide protection from unauthorised access, general user should also physically secure their mobile devices and removable media.

4. Data Loss Reporting

In case of any loss or theft of devices and media, user should report to the IT department immediately for any remediation and follow-up actions.

Conclusion

To achieve all-rounded security of the IT environment in the university, data encryption plays an important role to protect sensitive information. Management should gather requirements, identify constraints and define appropriate solutions to implement data encryption within their universities.

General users should be well aware of their own responsibilities towards data encryption and comply with relevant policies and procedures established by management to prevent the confidentiality, integrity and availability of sensitive data from being compromised.

Related Article

Campus Encryption Standard of Minnesota State University

Acceptable encryption algorithms for government data are outlined in the Federal Information Processing Standard 140-2 (Security Requirements for Cryptographic Modules). Encryption products must be validated by the Nation Institute of Standards and Technology as complying with FIPS Publication 140-2 at any level. Approved standards for encryption, hashing, digital signatures, random number generating, and message authentication include: AES, 3DES, Skipjack, DSA, RSA, SHA, CMAC, CCM, HMAC, and MAC. (http://www.mnsu.edu/its/security/encryption_standard.pdf)

Related Article

Encryption technologies: testing and identifying campus needs

Lehigh University is implementing a plan to secure sensitive information across campus through the use of various encryption technologies. Several committees were formed, at all levels of the University, to advise, identify, and direct data security activities at the enterprise level. One of these committees was assigned to take a detailed look at the types of hardware and media that need to be secure, to test various encryption technologies and hardware devices, and to produce a recommendation on which technologies needed to be implemented. (http://portal.acm.org/citation.cfm?id=1294071&dl=ACM&coll=DL&CFID=115226856&CFTOKEN=26659571)

Reference:
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf
http://www.truecrypt.org/
http://www.winzip.com/index.htm