Encryption Security - a necessity or requirement?

A secure computer environment would not be secure without consideration of encryption technology. If encryption is not used, it is just a question of time before hackers break into computer systems, bypassing the existing defenses and compromising data. But how important is encryption to an organization's security?

Various statistics and surveys show that encryption is becoming a more and more important security feature in today's world. An annual survey of Ernst & Young in 1996 showed that 26% of all surveyed information security managers used file encryption, 17% telecommunications encryption, and 6% public-key cryptography. In the same year, Trusted Information Systems of Glenwood, Maryland listed 1393 encryption products created and distributed by 862 companies in at least 68 countries. About 60% were from the US. The rest were produced in 28 other countries.

Although the encryption market appears to be growing and many companies are using encryption as part of their security system, there are many issues corporations need to consider before using and implementing encryption systems. This analysis will focus on the advantages and disadvantages of encryption as a corporate security solution and the challenges corporations face when dealing with encryption implementation and security regulations.

Encryption in the most cases is used to send sensitive or confidential electronic data to another system or location (47%). Only 31% of surveyed companies encrypt data on a computer storage device and only 24 percent use encryption for backup files or tapes when sending them to offsite locations or archives. The reason for this is, according to Jeff Montgomery, that although the encryption market is flooded with many solid encryption solutions, they address encryption only at certain points. These products might help encrypting data in files or during transfer but not within database structures, such as files that are located within a database. Solutions that can handle both are very demanding in, not only technical but also implementation, maintenance, resources and price.

The primary reason why companies hesitate to implement encryption solutions is the concern about system performance (69 percent) followed by complexity (44 percent) and cost (25 percent). Not only is that a valid argument but many companies are concerned about data loss during or after encryption has been implemented. If the implementation or the encryption is not properly planned and realized, the data integrity might be jeopardized, which might cause not only data but also great financial losses.

One of the main aspects corporations have to analyze when considering an enterprise wide encryption implementation are the surrounding business issues. These include the cost and technical support for implementation and maintenance. Data encryption in today's enterprise is very complex. It requires deep technical knowledge, most times additional hardware and software and demands ongoing management, an enterprise solutions approach, and a careful hand. As corporation grows and need change, costs of encryption will increase and system might have to be upgraded or replaced with a new and compatible solution.

The hardest tasks which business people and their professional IT consultants face, is to find out which encryption product is suited for which purpose. The various systems have many good “qualities” which range from good encryption, which has never been broken and never will be, to encryption that looks very scrambled, but can be broken by an expert in a few minutes with a pen and paper. Other encryption products are being judged by sales talks as well as on the prestige of the company name.

Although encryption technology in the 90's was very popular and primarily used as end-to-end technology, where it was run from the edge of the network, Chief Information Officers (CIO's) saw this technology more as a "bug" rather than an enhancing feature. These services were high in training and installation costs and carried many technical problems. One of these problems was that encryption made it harder for network diagnostic tools to penetrate and analyze the corporate traffic flow. Eventually other security products came along, and drew more enthusiasm than encryption systems. One if the main products were firewalls and intrusion detection systems, which did not demand as many technical and manpower resources for installation and administration. "Crypto companies were begging for someone to pay attention to them," remembers Vin McLellan, managing director of the Privacy Guild, a security consultancy in Chelsea, Mass.

Before starting implementation, companies have to look at the pros and contras for using encryption solution as corporate tools. Security concern is growing and corporations and their employees see a need for it and feel more secure when using encryption to send sensitive or personal data. This is a main reason why many corporations are evaluating and considering encryption systems. But also, there are many companies and institutions, which are "forced" to implement encryption to protect customer data and transactions to oblige by all current laws and regulations. In the past years, government has passed many new laws and regulations, governing security. PCI, SB 1386, GLBA, and SOX have evolved into much more than simply security and regulations related acronyms. They are the drivers for encryption in today's security world.

According to latest security studies, the main reasons for implementing encryption solutions are to prevent data breaches (55 percent), protect the company’s brand or reputation that could result from a breach (40 percent), to comply with security regulations such as Sarbanes-Oxley (49 percent) and to avoid having to notify customers or employees after a data breach occurs (12 percent). Other important regulations that are in place and influence corporations to implement encryption solutions are various state and emerging federal regulations on data security breach notification (57 percent) and HIPAA (43 percent).

Just like the commercial sector is using encryption, various government agencies as well as the military began to implement encryption and PKI systems on a “regular” level than just for communication and transmission of classified data as it has been in the past. Encryption is being used to transmit personal data on government websites, while filing taxes or requesting information. But at the same time tough, the same technology that allows to securely send information across the Internet and e-mail, makes it harder for law enforcement authorities to detect terrorist plots or build cases against criminals.

Research shows that many professionals view encryption as an important security tool - a tool that enhances the information security and overall sense of trust or comfort in their organizational data protection efforts. Despite the fact that many companies implement encryption to comply with latest security regulations and laws, there is a motivation to prevent a security breach and protection of the organization’s brand and reputation. This suggests that organizations are realizing the importance of raising the bar in the area of data protection in order to maintain the trust and confidence of individuals who are providing their personal information. And although there might be valid arguments against using encryption such as the extensive knowledge and new technology required, there is little contra, that the best way to protect data is to encrypt it by using a strong encryption and managing the encryption keys properly.

By Dasha Deckwerth
Stealth - International Intelligence Security Service Inc.
www.stealth-iss.com

About Stealth - ISS® Inc.

Stealth - ISS®, headquartered in Tampa, FL., is a privately owned Information Technology security consulting company with main focus on regulatory compliance, security integration, security consulting and managed security services for both government and commercial customers.

Founded in 2002, the company has earned an outstanding reputation for professional security services including vulnerability assessments and regulatory compliance such as Sarbanes-Oxley, HIPAA, NIST and ISO standards. Stealth – ISS® also recently expanded its data center services providing faster and secure hosting and colocation solutions for customers worldwide.

Stealth - ISS® has partnerships with several leading manufacturers of various security applications and products and was awarded the NATO BOA agreement in 2003.

About the Author

Dasha Deckwerth is the CEO at Stealth - ISS, with extensive experience in international business and computer security. Prior to her position as CEO, Dasha had gained extensive international business experience in various European, Asian and Central American countries and later became the VP of Marketing and Business Development at Stealth - ISS® in Berlin, Germany. She also worked on several projects as security and regulatory compliance consultant in the commercial sector as well as for various NATO countries and government agencies. Dasha’s current focus includes managed data center services, knowledge management, regulatory compliance applications and services and security implementations and consulting. Mrs. Deckwerth holds a B.A. in International Relations and Foreign Affairs from Eckerd College, is currently pursuing an MBA in IT Management from Touro University and speaks six languages.