A HURWITZ WHITE PAPER

Establishing a Data-Centric Approach to Encryption

Marcia Kaufman, COO
and Principal Analyst

HURWITZ
& ASSOCIATES
Insight to Action

Sponsored by Voltage Security

Voltage Security: Establishing a Data-Centric Approach to Encryption

Many data breaches occur at companies that already have a data security policy in place. While some of the millions of stolen credit card numbers have been easily lifted from unsuspecting companies with unprotected data, an increasing number of companies implement data security technology and find they are still at risk. These companies understand how important it is to keep their data assets safe from unlawful and malicious intrusion. As a result, they have a strategy for protecting their physical and digital perimeters. However, their data protection strategy is flawed. What is the problem and why do you need to make it a top priority to evaluate your current data security strategy? Typically, intrusion detection and other technologies designed to keep intruders out of your system are built to protect against previously known hacking strategies. This approach exposes your IT systems to great risk as new methods of intrusion are constantly being devised.

Typically, intrusion detection and other technologies designed to keep intruders out of your system are built to protect against previously known hacking strategies. This approach exposes your IT systems to great risk as new methods of intrusion are constantly being devised.

This paper will provide an overview of the evolving approaches hackers use to steal private data and describe the key requirements for protecting corporate data assets with a data-centric encryption strategy.

Understanding hacking strategies

A great deal of information was learned about the IT system intrusion methods of Albert Gonzalez and his global computer crimes organization when he was prosecuted and convicted in 2010. His organization was responsible for stealing millions of payment card accounts from retailers like TJX, Target, JCPenney, and Sports Authority, and food chains like 7-Eleven and Hannaford. These criminal hackers constantly evolved their methods and became highly skilled at locating vulnerabilities in the systems they tried to enter. They found ways to enter these systems and access company databases and applications. They were initially very successful at stealing credit card numbers by exploiting the vulnerabilities of early Wi-Fi networks at large retail companies. They sat in cars outside the building and easily hacked into sophisticated computer systems. A more advanced technique leveraged vulnerabilities of the software language used by most companies to connect their websites with data stored in their company databases - Structured Query Language (SQL). Now instead of sitting in a parked car outside a store, thieves could be located anywhere in the world and hack into a database through a website. And yet another evolution of the hacking process occurred when the criminals learned how to access credit card data from point-of-sale terminals. This meant that they could siphon off the credit card data every time a customer made a credit card purchase at one of these terminals.[1]

Many of these data breaches occurred over a long period of time. The companies were not even aware that there were intruders in their system until the damage was done – personal information stolen and company reputation severely

1 James Verini, "The Great Cyberheist," New York Times, 10 November, 2010

HURWITZ & ASSOCIATES
Insight to Action

damaged. The cost of damage control and other expenses for cleaning up after these breaches has been astronomical. The affected companies and others have been able to learn from these thefts and have implemented technology to help protect against criminals who use similar intrusion methods. Unfortunately, these data loss prevention strategies often give companies a false sense of security. For example, a company with an online sales channel uses sophisticated security technology designed to protect customer data in the tunnel between the browser and the company's servers. However, as the company has increased its use of cloud computing, wireless technology and mobile devices, its corporate boundaries have opened up dramatically and their data is still very much at risk. There are many new ways to enter their system and new methods of security are required.

… hackers are becoming familiar with breaking the code of security keys as well. In 2011, Lockheed Martin and Sony Corporation suffered security breaches that appeared to compromise their security key systems.

Information security needs to protect against known threats as well as against those threats that are currently unknown. Intruders are able to create new methods for unlawful entry faster than you can devise new strategies to block them. As a result, various methods used for authentication, monitoring, and otherwise protecting the perimeter from intrusion are no longer sufficient. These IT security strategies are a first line of defense and they leave your data vulnerable if they fail. Therefore, it has become increasingly important to implement a data-centric approach to encrypting and securing data that helps you to lock down your data and keep it safe wherever it goes, however it is used, and throughout its lifecycle. You need to secure your data based on the assumption that hackers will find a way to bypass your identity and perimeter protection technology. Or for an even scarier thought, you need to assume that hackers may be lurking in your system now waiting for the right opportunity to steal private data under your control.

Using encryption to protect your data

Some of the data stolen by criminal hackers like Gonzalez was unencrypted and, therefore, easily understood once it was accessed. Many companies now use some form of encryption to provide added security, but hackers are becoming familiar with breaking the code of encryption keys as well. In 2011, Lockheed Martin and Sony Corporation suffered security breaches that appeared to compromise their security key systems.

Encryption is a way to scramble information so that it can only be understood by people or machines who posses a unique key or pass code. This protected information must be easily recognized and processed by IT systems and business processes, but not by hackers. Unfortunately, not all encryption methodologies are the same. It has become increasingly important to understand which type of encryption you have deployed and if this is the best approach for your environment. There are many different ways to use encryption as a security tool and there are many variations on how passcodes or keys are created and used. It can be challenging to ensure that your encryption keys are sufficiently complex making it hard to break the code, and at the same time simple enough so that authorized users can access the protected data when needed.

HURWITZ & ASSOCIATES
Insight to Action

Encryption has been used to protect data when it is at rest or stored in some type of container. The data needs to be unencrypted when you need to use it to complete a transaction or business process. Examples of this type of encryption include:

- Database encryption – To protect against a data breach from hackers gaining entry to internally stored data
- USB stick encryption – To protect against sensitive data being accessed from a USB stick that can be easily lost or stolen
- Backup tape encryption – To protect against sensitive data being stolen from backup tapes that could be stolen or lost when moved or stored
- Hard drive encryption – To protect against sensitive data being stolen from a laptop carried by an employee

One of the long-standing weaknesses with encryption strategies is that your data is at risk before it is encrypted and after it is decrypted.

Key considerations for implementing a data-centric encryption strategy

The encryption methods described above only protect data when it is at rest or stored in a particular container. However, these methods do not protect your data wherever it travels. One of the long-standing weaknesses with encryption strategies is that your data is at risk before it is encrypted and after it is decrypted. For example, in a major data breach at Hannaford Supermarkets in 2008, the hackers hid in the network for months and were able to steal payment data when customers used their credit card at the point-of-sale. This breach took place before the data was encrypted. In another retail example, customer personal data was securely encrypted in the database, but was decrypted at the time of the transaction in order to verify customer information. While the company met its PCI (Payment Card Industry) data security standard compliance requirements for data storage, its data was not adequately protected. When the customer made a purchase online, his address and credit card information was tested for accuracy and during this time it was brought out of the protected tunnel for a split second. This is all the time a sophisticated hacker needs to pilfer this information from the IT system. In each of these situations, the company complied with PCI requirements, but they left some gaping holes in their data security strategy. The thieves were able to identify these weak points and steal data that the company thought it was protecting. The key considerations for encrypting your data so you can provide more comprehensive protection are as follows:

- Protect data at rest and in motion. If your data is encrypted only when it is in a database or other container for storing data, then your data becomes vulnerable when it is transported or used to complete a transaction. A hacker can infiltrate your system and steal data when it leaves your database and becomes decrypted.
- Encrypt data for as long as possible. Your data should be encrypted as soon as it is collected and should remain encrypted for as long as possible. The data should be decrypted only when it is actually necessary to complete a business process. For example, you would need to decrypt the data when processing

HURWITZ & ASSOCIATES
Insight to Action

a charge back. In order to keep your data encrypted as long as possible you will need a key management process that automates the process of verifying identity and access rights.

- Process data while it is encrypted. As hackers continue to discover additional vulnerabilities and ways to steal data when it is decrypted, the most secure approach is to process data while it is encrypted. This is not a practical approach when deploying traditional encryption methods. These traditional methods significantly change the structure and format of the data making it time consuming and costly to incorporate encrypted data into existing applications. However, if you use an encryption method that allows you to maintain the format of the data, then you will be able to process data while it is encrypted without making costly changes to your applications.
- Encryption keys need to be computed as needed. The management of encryption keys can get very complex. For example, as companies begin to deploy hybrid cloud environments - including virtual data centers and private and public clouds - they need to add more encryption keys. In addition, additional encryption keys may need to be added for companies trying to secure data as it moves between traditional corporate boundaries and the mobile devices of customers and partners. Simply adding more keys is not the answer. Maintaining a large number of keys is impractical and it is hard to manage the storing, archiving, and accessing of the keys. In order to alleviate this problem, encryption keys should be generated and computed as needed to reduce complexity and improve security.
- Encryption keys need to be protected. Criminal hackers understand key management and are beginning to target this type of security protection. Having a security key is not sufficient protection. The key itself needs to be protected on its own and separated from the data.

… if you use an encryption method that allows you to maintain the format of the data, then you will be able to process data while it is encrypted …

Voltage Security Solution

The Voltage Security data encryption platform and key management process incorporate the characteristics for a data-centric approach to encryption described above. The company's security solutions are based on its two innovative encryption technologies: Identity-Based Encryption (IBE) and Format-Preserving Encryption (FPE). IBE protects data so that only a specific person or machine can access that data without requiring the complexity of traditional approaches to encryption. Instead of using long, randomly generated keys that must be mapped to digitally signed documents, IBE relies on a key that does not need to be mapped to a certificate. This process significantly decreases the complexity while providing the level of security required. This encryption process can be used to secure email files, documents and databases without the need to pre-register recipients of the secured data. FPE protects structured data such as credit card or social security numbers without changing the format or structure of the data. This is a change from the traditional approach that turned credit card or social security numbers into very long strings of numbers. These long encrypted numbers would not work with a company's existing applications designed to process transactions or complete specific business processes. The Voltage solution is designed to enable the processing of data while it remains encrypted.

HURWITZ & ASSOCIATES
Insight to Action

Conclusion

By implementing a data-centric approach to encryption you can increase the security of your company's valuable data assets. Even with highly sophisticated IT security systems designed to protect your physical and digital perimeters, your data may still be at risk for a data breach. Therefore, you need to begin thinking about what you would do to protect your data if a hacker is already hiding and waiting in your IT system. In fact, one of the most important lessons from an analysis of previous data breaches is that the hackers are constantly evolving their methods. You need an approach to data security that does more than protect against previously identified threats. If a data thief finds a new way in to your system, you want to ensure that he is unable to do any damage and leaves empty handed.

In summary, in addition to your IT security strategy it pays to incorporate a practical approach to data security. Make sure that you only store data that you really need. If you do need the data, then you should encrypt it for as long as possible.

You need an approach to data security that does more than protect against previously identified threats.

HURWITZ & ASSOCIATES
Insight to Action

About Hurwitz & Associates

Hurwitz & Associates is a consulting, market research and analyst firm that focuses on how technology solutions solve real world business problems. The firm's research concentrates on disruptive technologies, such as Cloud Computing, Service Oriented Architecture and Web 2.0, Service Management, Information Management, and Social and Collaborative Computing. We help our customers understand how these technologies are reshaping the market and how they can apply them to meet business objectives. The team provides direct customer research, competitive analysis, actionable strategic advice, and thought leadership. Additional information on Hurwitz & Associates can be found at www. hurwitz.com.

175 Highland Avenue, 3rd Floor • Needham, MA 02494 • Tel: 617-597-1724
www.hurwitz.com