Defend Yourselves - We Are Under Attack

The world's landscape has changed forever

Contact Information

Steven R. Russo
Executive Vice President
Secure Cloud Systems, LLC
Phone: 1-719-555-5555 x120
Email: russosr@SecureCloudSystems.com
Fax: 888-344-6556
Web: www.SecureCloudSystems.com
www.certainsafe.com

Today, more than ever, there is no escaping the fact that everyone is vulnerable to cyber-attack. Everything that permits access and ease of use is now exploitable for hackers to attack. Personal information, financial assets, corporate intellectual property, power grids, government systems, and infrastructure are all under attack. We live in a world where the landscape is continuously changing bringing both convenience and insecurity.

Cyber criminals have experienced continued success in their attempts to exploit our Nation's sensitive data. Cyber criminals have infiltrated everything from our banking institutions to our Healthcare data. They have intercepted countless communications that are both sensitive and dangerous when fallen into the "wrong" hands. The risks associated with the current methods for protecting critical data from cyber-attack and exploitation are becoming increasingly apparent.

As individuals and collectively as a Nation, we must deploy effective, yet flexible, high-security solutions. These solutions must be capable of providing authorized control of critical information while simultaneously protecting the information, regardless of its location. This is no longer an option. This is a reality. We are under attack and it appears that the battle will rage on for the foreseeable future.

The Centuries Old Battle

Since the days of the castle and moat, we have patterned our approaches to security around a two-dimensional defense architecture that relies on a limited number of controlled, easily discernible access points. The more valuable the items to be protected, the greater the number of defensive layers we applied. First we built the outer wall, then the moat, drawbridge, gatehouse, inner walls, castle keep and so on. At each layer in the architecture, we placed greater restrictions on who was able to gain access.

Little has changed in this architecture. With the advent of the computer age, the castle and moat architecture was simply adapted into the IT environment. Firewalls take the place of mortar and brick walls while restricted use websites take the place of drawbridges. As technologies advanced and the cyber threats adapted, we continued to follow the castle and moat architecture by creating inner walls within outer walls through the use of more sophisticated web designs and virtual private networks.

It's time for change. We, the people, and our government, are losing the cyber battle. Malicious actors, both foreign as well as domestic, continue to have their way with our liberties and our quality of life. The way we conduct our daily lives is at risk today. We need to realize and accept that we must do more and it must be done now. In order to fight back in today's cyber battle, we need to take definitive action for the good of individuals and the Nation as a whole.

The best offense is a strong and all-encompassing defense. Cyber warfare has taken root within the past decade. New ways to secure critical infrastructure, privileged data, and all communications are now required for the protection of our livelihood and our freedom. One of our highest priorities as a Nation must be given to ensuring the security of sensitive data as well as communications of all types.

In The News

Feb 3, 2014 – Statement by American Bankers Association, The Clearing House, Consumer Bankers Association Credit Union National Association, Financial Services Information Sharing and Analysis Center, The Financial Services Roundtable, Independent Community Bankers of America, National Association of Federal Credit Unions. In all data breaches, including the recent retailer breaches, the financial services industry's first priority is to protect consumers from fraud caused by the breach. Banks and credit unions do this by providing consumers "zero liability" from fraudulent transactions in the event of a breach. Although financial institutions bear no responsibility for the loss of the data from a retailer's system, they assume the liability for a majority of the resulting card-present fraud. In most instances, financial institutions have historically received very little reimbursement from the breached entities.

Feb 26 2014 - "Tough as the 2013 holiday season was for many retailers, Wednesday's fourth quarter earnings report proves that few had it tougher than Target, which was bedeviled during the peak shopping season by one of the largest-ever retail data breaches. The company's long-awaited fourth quarter results tell a tale of woe: Net income fell 46% to $520 million, or $0.81 per share, from $961 million, or $1.47 per share, a year earlier," the Minneapolis-based company reported.

April 2014 - Michaels Stores has announced that around 2.6 million credit and debit card accounts may have been effected by a security breach. The breach may have exposed cards that were used at Michaels stores between May 8, 2013 and January 27, 2014. Michaels reports that the compromised data includes customer information such as payment card numbers and expiration dates.

August 2014 - Computer hackers targeted JPMorgan Chase & Co. (JPM) and at least four other banks in a coordinated attack on major financial institutions leading to the theft of customer data that could be used to drain accounts. Hackers targeted customer gigabytes of data and employee information. The scale indicates a potential for significant financial fraud.

September 2014 - Credit Card Breach at Home Depot - Multiple banks state they are seeing evidence that Home Depot stores may be the source of a massive new batch of stolen credit and debit cards that went on sale this morning in the cybercrime underground. "I can confirm we are looking into some unusual activity and we are working with our banking partners and law enforcement to investigate," Home Depot spokesperson Paula Drake confirmed, reading from a prepared statement. There are signs that the perpetrators of this apparent breach may be the same group of Russian and Ukrainian hackers responsible for the data breaches at Target, Sally Beauty and P.F. Chang's, among others.

The New Reality

The threat of cyber-attack, underscored by the recent amount of mass-data breaches in the financial sectors, are now so great that US financial institutions are rushing to buy insurance coverage against the expense of losing sensitive customer information. Cyber insurance has graduated from a faraway thought to somewhat of a necessity; however, obtaining insurance is not the answer to the root problem. The current imminent need is for new ways to secure data at rest and data in motion from cyber-attack, mass data loss, and internal as well as external criminal exploitations. “Companies of our size unfortunately experience cyber-attacks nearly every day,” Patricia Wexler, a JPMorgan spokeswoman, said in an e-mail.

The most powerful government agencies and corporations alike are terrorized with constant security breaches against their infrastructures. Both the private and public sectors of the economy are having increasing difficulty protecting sensitive information of all types.

Dynamic data-centric security solutions that “protect data at rest and data in motion,” even when a security breach of an existing network or data center occurs, must be considered a paramount requirement. We must not only protect from the outside in, but from the inside out. We must take the approach of understanding that it is not a matter of “if” an attacker breaks through our perimeter defenses but “when.” Once it occurs, how can a criminal be stopped from exploiting the crown jewels assumed to be within? Cyber insurance is not going to save your firm’s reputation. It is not going to mitigate the loss of credibility experienced in your business sector. It’s not going to stop the loss of business associated with the lack of trust created by the event. In the trenches of this cyber war, the only real insurance is to find ways to stop the events from occurring in the first place.

The Secure Cloud Systems Difference

Our mission is to deploy effective, yet flexible, cyber security solutions capable of supporting authorized access to privileged data and communications regardless of its location, service provider, or point of use. Sensitive information must be protected from both internal and external threats. An innovative solution needs to enable rather than inhibit information sharing, even when traditional information technology defenses are breached. The primary goal of providing impenetrable security for real-time information while achieving the cost savings potential of cloud computing requires a fundamental change to the “Castle and Moat” defensive architecture of today.

Finding new ways to secure sensitive data has never been more important. Data security must be all inclusive and support the full range of operations which include internal and external communications, financial transactions, client records, and data in storage. Around the globe, we face an ongoing challenge of how to safely store and transmit data securely while still maintaining easy access and not impacting ongoing business processes.

MicroTokenization® and MicroEncryption® Capability

Until now, bulk encryption, combined with firewalls, was the most effective solution for protecting data and other informational assets against internal and external threats. Encryption is the process of transforming information, plain or accessible text, into an unintelligible scrambling of code referred to as cipher-text. This process utilizes a secret key with an algorithm and is known as ciphering. The cipher-text, or encrypted data, is designed to be decoded, transformed, and restored back into its original readable form by utilizing the original cipher algorithm and a secret key. The intent of this process is to secure and protect critical information from theft and exploitation.

As previously cited, these defenses were not enough to protect Target Corporation or the financial data of its customers. In order to fill these types of security gaps, Secure Cloud Systems has developed a next-generation data security solution that virtually eliminates the loss of sensitive data. MicroTokenization® and MicroEncryption® secured products and services (Certified to PCI Level 1 DSS) are immediately available to secure networks, information systems, the banking and financial communities, government and military, as well as other forms of privileged communications.

Continuous Innovation and Architecture

Advanced data-centric cybersecurity methods beyond DSS PCI Level 1 standards should be designed to be easily configurable. An honest assurance must be given that those levels of security, unattainable with traditional network defenses, have indeed been developed and deployed. Methods to not only mitigate, but eliminate the mathematical probability of a mass data breach are critical. In short, a new way to secure and store sensitive data is no longer an option, but a mandate. The requirements established by Secure Cloud Systems will ultimately change the way data is stored well into the future.

Summary

A need for a new and innovative security paradigm is evident. Protecting all forms of data in the unfortunate event of a perimeter defense breach is no longer optional. Twenty-first century information sharing requires trusted, self-sufficient secured data backed by the best technology. This technology must provide full assurance that the information is genuine, unaltered and completely trustworthy and unavailable to internal or external exploitation. This new paradigm must ensure that only the right people get access to the right information at the right time. Architectures such as those offered through Secure Cloud Systems MicroTokenization® and MicroEncryption® capabilities can achieve that goal. They provide those assurances that data at rest and data in motion remain BLACK and unavailable to exploitation even in the event of a traditional network defense breach. Defending our world that's under attack has now become the new normal; our world whose landscape has indeed been changed forever.