Health IT Security Journal

Volume 3, No. 2

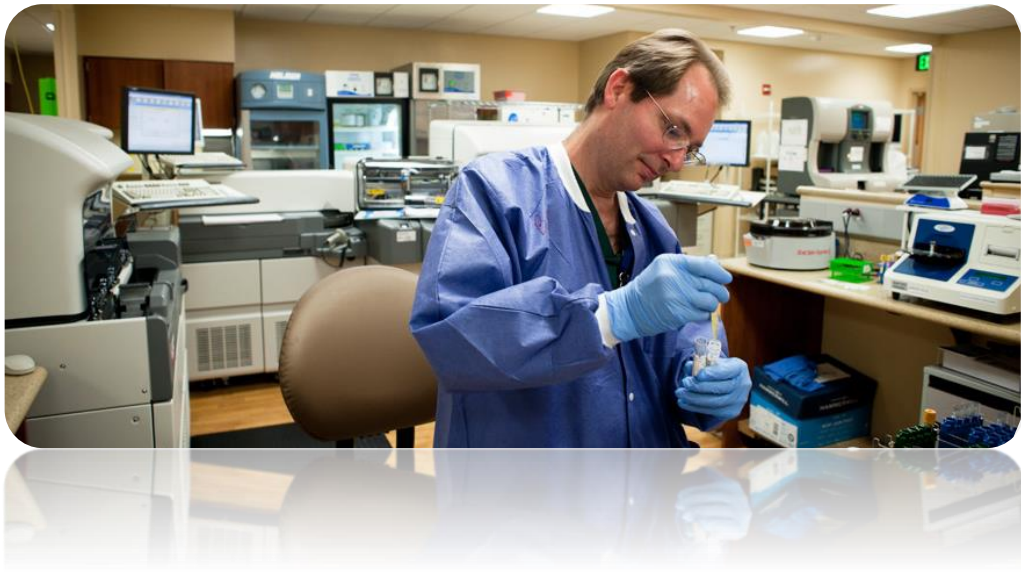
How to Build an Effective Security Team

The Art of Cryptography

A publication of the HITSF

Health IT Security Journal

Volume 3, No. 2



HITSF

IN THIS ISSUE

This journal is a publication of the Health Information Technology Security Forum.

The Health IT Security Forum is an International Security Organization that dedicated to help healthcare organization in securing their privacy data, confidential information, medical devices and will be recognized for the passion of its members in conducting multidisciplinary research and development in the area of Healthcare IT Security and e-Health.

Letter from the editor

Dear readers,

This is the second year of the Journal and we are proud to present another issue. This issue of the HITSF journal offers insight into information security for healthcare practitioners. We hope you will enjoy it and we welcome your feedback. Please send questions and feedback to editor@healthitsecurity.org

- Hadi Syahrial

Disclaimer

The author(s) of each article appearing in this Journal is/are solely responsible for the content thereof; the publication of an article shall not constitute or be deemed to constitute any representation by the Editors that the data presented therein are correct or sufficient to support the conclusions reached or that the experiment design or methodology is adequate.

www.healthitsecurity.org

How to Build an Effective Security Team

by Eric Vanderburg

The best security team should be able to protect your most prized possessions, assets and interests. In the business world, security can mean protection of office premises, employees and clients. Because this covers a wide range of aspects, it is only right that people who make up your security team come from different departments.

But who should be part of your security team?

Executive leadership

Effective security teams have top level support through a member of the C-suite. Their leadership role will prove beneficial to the group, not to mention their thoughts on the security system developed and installed. It is vital that they believe that the system is cost-effective and will not disappoint.

IT staff

These days, an office's security system is linked with the information systems' infrastructure of a company, which means they go hand in hand. Security breach, after all, not only happens offline, but also online. Nowadays, you not only need to keep an eye on who walks through the door, but also on who has access to your network. This only shows that a member of the IT department must be included in a security team, whether security system is managed in-house or outsourced.

It is important to note, however, that the IT department should not dictate which security system should be used company-wide. They should take care of the virtual security and leave the physical security to the security department.

Human Resources

Who better knows employment laws, company policies and other labor rules than human resources (HR)? They can help ensure that the security team is not violating any laws when they developed or implemented a system. Moreover, there is an important link between security and HR where employees are concerned. The moment a new hire is onboard, he will be added to the security system right away. If anyone gets fired, he will be removed from the system just as quickly. HR is also responsible for creating security measures, such as questioning anyone without a name badge or prohibiting them from accessing certain areas of a storage network.

Finance

Apart from the fact that money is needed to implement a security system, a representative of the finance department will also ensure that the plan made and the steps taken will have a positive impact on a company's bottom line. Security, after all, is not the only thing that a business has to spend on. It is vital that the security system implemented proves to be a lucrative investment, rather than a money pit.

Now that the team members have been selected, it is time to take the steps to ensure a security team functions as intended.

Security challenges must be identified, so solutions to address them will be formulated.

Reduce security risks, such as online and offline breach.

Perform ongoing and regular maintenance.

Choose a system that provides most value, and can be leveraged across multiple departments.

About the Author:
Eric Vanderburg

Director, Information Systems and Security, JurInnov Ltd.

Eric Vanderburg understands the intricacies inherent in today's technology and specializes in harnessing its potential and securing its weaknesses. He directs the efforts of multiple business units including Cyber Security, eDiscovery, Computer Forensics, Software Development, IT and Litigation Support at JurInnov, an eDiscovery and eSecurity consulting firm. Vanderburg holds over thirty vendor certifications and is completing a doctorate in information assurance. He has dedicated much of his career to designing and implementing systems, policies and procedures to enhance security, increase productivity, improve communications and provide information assurance. He has been invited to speak at conferences and events on technology and information security and he is active in promoting security and technology awareness through various publications. Look for his latest book, "Storage+ Quick Review Guide", due for publication with McGraw Hill in December of 2013.

The Art of Cryptography

By Neha Verma

Understanding technology and computer encryption is essential in today's world of cyber attacks and security breaches. Have Paper Masters custom write a research paper on exactly what encryption is and how it is used today. You tell us what type of encryption you want to focus on and our writer will compose a project exactly how you need it to be.

Encryption is a form of cyber security created by altering information before transmission, so that only an authorized sender and receiver can encode and decode the information. It is a effective form of information security.

While the technology that enables encryption to code and decode messages sent over telephone lines is a product of the late twentieth century, encryption has been around for centuries, most notably as a province of war rather than commerce. As early as the 5th century B.C., the rulers of Sparta employed a cipher device called a scytale to disguise communications of an official nature that for delivery by courier. If intercepted by an enemy, it was unreadable. This method of security protected vital information from reaching enemy hands for centuries.

Encryption remained a pencil and paper technique up until World War Iwhen machines began to be used to code information. These electronic mechanical devices both produced strong ciphers and increased the speed of encoding and decoding. They eventually gave way to the construction of the world's first digital machine.

Following the World War II engineers began to experiment by programming computers with ciphering and enciphering technology, marking the advent of electronic encryption. Like virtually all such techniques since Caesar's time, the new electronic encryption was primarily utilized to keep military secrets. However, as one author notes, the use of this technology changed dramatically in the late 1970s and early 1980s when organizations other than the government began transmitting sensitive information over phone lines.

While most encryption attacks have proved themselves to be harmless attempts to prove the weaknesses of advancing encryption methods, the implications of both proffered and clandestine attacks has demonstrated that more secure methods and techniques of encryption across networks is imperative. Nevertheless, until fail-proof techniques are developed, businesses, private users and the government alike continue to take advantage of the safeguards that encryption currently affords.

The underlying concept and purpose of encryption as it pertains to all types of transactions across networks of any sort is the ability to transmit such transactions with the confidence that they cannot and will not be intercepted and viewed by anyone other than the intended receiver. In essence, encryption allows for the adequate coding of a message or transaction along a network by a sender and the subsequent decoding of such message by no one other than the receiver.

To facilitate such a transaction, the following steps are taken:

1. A key must be exchanged between the sender and the receiver to decrypt encrypted messages.
2. This key is used to both encrypt and decode messages between the two.
3. A single secret key or symmetric cryptosystem can be used, which also has the capacity to secure or protect files on a user's personal computer.

While this technique is more than efficient for non-commercial purposes, the security and transmission of commercial or highly sensitive information requires stronger encryption methods.

Symmetric key encryption uses a single key for the coding and decoding of information. The algorithm in this case is made public or exchanged between recipient and sender, which requires special attention that the key remain confidential to only those participating in the exchange of information. An

intercepted message remains secure only as long as the key is held by the appropriate sender and recipient.

Asymmetric encryption uses two keys, public and private to secure the transmission of information, and which are created by a single user. The user has sole access to the private key but may distribute or publish the public key. Each key plays a role in encoding and decoding the text of a message. Asymmetric encryption offers the advantage of not having to exchange a secret key however the lengthy mathematical computations required for encryption make it impractical for sending large messages.

This limitation has been addressed by the combination of public key encryption and secret key distribution. In this case, the sender can encrypt the message's secret key with the recipient's public key and append it to the encrypted document. Security is maintained because the sender also digitally signs the message, which proves that it originated from the sender. This technique is unique in that it uses a authentication to provide an even greater level of security.

In a comprehensive white paper on the security threats of distributed computing, author Andrew Twyman details the concentrated power that parallel computer offers in cracking the encryption techniques used under several network protocols. While Twyman concedes that parallel computing is not a new concept, its role as a vehicle for encryption cracking is a relatively new phenomenon and "lends itself very easily to this method of attack".

Surprisingly, one of the first concerted efforts for breaking RSA encryption techniques was an official call for challengers in a contest to test RSA factoring in 1991. An SSL challenge followed in 1995, which was especially significant in that it focused on the burgeoning capacity of the World Wide Web as a medium for secure information exchange. Challengers were instructed to "crack a web session with Netscape's SSL encryption based on the RC4 stream-cipher with a 40 bit key". Clearly, the purpose of this challenge was to determine the potential fallibility of the current encryption systems, which it did in approximately eight days. The encryption system was undermined by two challenging efforts that utilized parallel machines and locally distributed systems.

Twyman suggests that the increase in both computer and Internet use makes a fertile groundwork for the potential misuse of parallel and distributed computing, especially for distributed encryption cracking. At the same time, he points out that encryption cracking is often a random process that relies on finding a single, unknown key rather than a search for a specific key used in a specific algorithm.

Twyman also suggests that single keys are the most vulnerable to attack and present the greatest weakness in parallel computing methods. Used primarily in the transmission of email messages, single keys are adequate for handling less sensitive information however if a session should include a login ID and password, especially of a networks system administrator, the implications for a system breach and damage become even greater.

About the Author:

Neha Verma

Neha Vermais a researcher and faculty at Gujarat University.