BE FREE

CASE STUDY

BE FREE OF RISK

Developing a Playbook to Keep Systems Secure

A government hospital worked with BestIT to fill the gaps in their IT security.

Briefing

A major county hospital was overdue for vulnerability testing of their IT security infrastructure. They thought that they had the latest security parameters in place to protect patient data from any form of security breaches. The BestIT security team discovered and exploited major vulnerabilities in their network. A plan was put in place to seal them and strengthen their security.

BE FREE

Developing a Playbook to Keep Systems Secure

Client
Government Provider of Health Services

Industry
Hospital - Public Health Services

Challenge
After a three year hiatus, the hospital needed to undergo vulnerabilitiy testing to identify the gaps in its IT security infrastructure. The IT department was concerned that not enough was being done to protect more than four million patient records it handled each year.

Services Provided
- Vulnerability Testing
- Limited Penetration Testing — Internal and External
- Limited Policy Review

Benefits
- Realistic assessment of their ability to defend against a state of the art attack
- Prototype for a new password policy
- An unbiased description of their state of risk which will enable them to reevaluate their IT security infrastructure

Introduction

When you process more than four million patient records each year, having an effective security strategy in place is important to protect the confidential information that passes through the servers each year. After a three year vulnerability testing hiatus, the IT team at the county hospital knew that gaps might exist within its current security infrastructure but weren't sure of the depth of those security gaps. They knew more could be done to enhance the security parameters and controls at the hospital but they needed to pinpoint where the greatest risk existed with the IT security envrionment. BestIT was called in to provide a candid report of their securty state to help drive organizational change.

The Problem

The hospital had perviously outsourced their vulnerability patching to a vendor that underperformed. They had a vulnerability scanner that couldn't detect that the patches put in place were ineffective. The client was struggling with controlling the potency of the tools used to strengthen their IT security. They knew that the information security department and at the hospital was underfunded and needed a plann to focus on improving and strengthening the security environment at the hospital. In addition, they wanted to know what their security tools were not capable of doing.

The Solution

To start, BestIT met with the chief privacy officer of the hospital to determine the effectiveness of their minimum password policy per HIPPA guidelines. Once that was completed, BestIT began the vulnerability assessment and internal and external penetration testing.

The Results

By the second day of the assessment, BestIT had full control of their IT security environment due to weak anti-virus software. BestIT security architects were able to take control of 365 different computers on the network using different hacking methods. The hospital's technology successfully defended them against a wireless attack but procedural probelms with identity management and patching issues left their securtiy infrastrcutre vulnerable. In addition, a live intrusion was performed for members of the IT department to show that their firewall could not successfully block an advanced hacking attempt. From an internal persepctive, the hospital wasn't able to see the advanced hacking attacks from their internal

Determinging cognizance of employee negligence

Employee negligence plays a role in data security for all organizations. BestIT wanted to test the level of security awareness of the hospital's IT employees. Working with the client, the BestIT security and marketing team worked together to create a fictious pizza company for demostration purposes at the hospital's headquarters. The team found a restaurant for sale across the street from the facility in the food plaza and sent out an email campaign featuring a full menu and address to the ficticious pizza parlor to 10 users in the IT department at the hospital. The deal offered them a limited time $1.99 pizza slice and a drink to show appreciation for their work as civil servants. The link to claim the deal was filled with benignly hostile code that would allow the BestIT security team to obtain password information once they clicked to claim the deal.

The campaign had a 10 percent success rate. However — BestIT experts were not able to download any password information because the employee accesed the link on a personal tablet using a different operating system that was not connected to the hospital's network.

controls. Since the firewall and anti-virus failed, security experts at BestIT were able to retrieve 13,000 password images on the network—some were active and others were not.

Overall the websites for the hosptial were mostly secure and so was the VPN. While no sensitive patient information was found on the website, newsletters featuring biographies about staff members, photos and digital signatures could result in employees being profiled from a spear phising attack vector. The county hospital now knew all areas of security it needed to address.

BestIT put together a report with all of the findings and recommendations on what to do next to close the gaps discovered in their security.

Conclusion

By allowing BestIT to perform a vulnerability assessment and review their password policy, the hospital now knew what to focus on to strengthen their security and add addtional layers of protection to patient records and other confidential data. They had all the information they needed to develop a playbook to enhance passwords at the organization, revisit their policy to prevent leakages when employees leave the organization and add an enhanced intrusion detection sensor to the security envrionment. Contact BestIT today to see how we can help you keep your systems secure.

Contact us for more information.
BestIT HQ
3724 N. 3rd Street
Phoenix, Arizona 85012

+1.877.222.8615 | info@bestit.com
www.BestIT.com