Analyzing the Vulnerability of U.S. Hospitals to Social Engineering Attacks: How Many of Your Employees Would Share Their Password?

B. Dawn Medlin, Appalachian State University, USA
Joseph A. Cazier, Appalachian State University, USA
Daniel P. Foulk, Appalachian State University, USA

ABSTRACT

One of the main threats to keeping health information secure in today’s digital world is that of social engineering. The healthcare industry has benefited from its employees’ ability to view patient data. Although access to and transmission of patient data may improve care, increase delivery time of services and reduce health care costs, security of that information may be jeopardized due to the innocent sharing of personal and non-personal data with the wrong person. Through the tactic of social engineering, hackers are able to obtain information from employees that may allow them access into the hospitals networked information system. In this study we simulate a social engineering attack in five different hospitals of varying sizes with the goal of obtaining employees passwords. 73% of respondents shared their password. This raises serious concerns about the state of employee security awareness in our healthcare system.

Keywords: healthcare; HIPAA; passwords; security; social engineering

INTRODUCTION

Health care records generally include, but are not necessarily limited to, individual patient’s health history, diagnosis, laboratory results, treatments, and the doctor’s progress notes. A patient’s personal information, such as address, phone number, and social security number, are all items that may be included and accessible to some or all health care employees. These records are vulnerable to security breaches and theft. Both hackers and social engineers have successfully found ways to penetrate networked health data systems by simply asking for the information or by finding weaknesses within the system.
Unfortunately, the largest threat to a health care agency’s security may not be outsiders, but rather their own employees. Inside employees actually can pose the largest threat to the security and privacy of information as they can exploit the trust of their co-workers, and they generally are the individuals who have or have had authorized access to the organization’s network and who are familiar with its internal policies, procedures, and technologies. Additionally, internal employees can exploit that knowledge to facilitate attacks and even collude with external attackers (http://www.cert.org/insider_threat/).

It is even more important today for health care providers to keep a patient’s information safe and private than ever before due to increased regulations and the increased opportunities for exploitation that exist in today digital world. Governmental agencies have adopted initiatives that specifically address the issues and rights of health care patients. More specifically, the security and privacy of health care information is protected by the Health Insurance Portability and Accountability Act (HIPAA), requiring health care agencies to do everything possible to protect their information.

There are many threats to the privacy of a patient’s information, and one of the largest threats is social engineering. Social engineering is generally defined to include the use of trickery, personal relationships and trust to obtain information; more specifically, it is the art of deceiving people into giving confidential, private or privileged information or access to a hacker (Gragg, 2007).

In our study, we simulated how a social engineer might gather information from unsuspecting hospital employees. Health care employees must be especially vigilant in their efforts to guard their passwords, as many have access to personal and medical information. HIPAA regulations are very definitive and have specific standards related to security and privacy of information; infractions of those regulations can be costly to the organization and its reputation, as well as devastating to a patient.

LITERATURE REVIEW

A patient’s medical record may include gender, race, family history, sexual history including types of birth control, sexual activity and treatment, any history or diagnosis of substance abuse, and diagnosis of mental illness. Other medical information, such as HIV status, may also be included. The accessibility of this confidential information may open the door to various forms of discrimination. For instance, chronic diseases such as HIV and AIDS may result in an increase in insurance rates or even denial of coverage, due to the usually extensive medical treatment needed. Some individuals may even be ostracized or stigmatized because of their disease type. Patients expect the information contained in their records to remain secure and private and seen only by those individuals whose access is medically or administratively necessary.

There is also a great concern about health identity theft, where people steals someone’s medical identity and uses their insurance for care. Not only can this be very costly to the one paying the bill, but it can also be life threatening because their medical records are inaccurate and may contain false information that might lead someone to give the wrong medications or treatments (http://www.naturalnews.com/020528.html). It is estimated that over 250,000 Americans have had their medical identity stolen and misused and that someone can by a health identity for as little as $60 on the street (http://articles.moneycentral.msn.com/Banking/FinancialPrivacy/DiagnosisIdentityTheft.aspx)

HIPAA regulations were enacted to protect the privacy and security of patients and their medical records; simply put, they make it illegal for unauthorized personnel to access or release information from someone’s medical records. More specifically, HIPAA addresses security and privacy measures in relationship to passwords, either directly or indirectly, in the following standards (http://www.hhs.gov/news/facts/privacy.html). These standards, as listed below, include management processes, user education and training, and access control.
Towards Usable Application-Oriented Access Controls: Qualitative Results from a Usability Study of SELinux, AppArmor and FBAC-LSM
www.igi-global.com/article/towards-usable-application-oriented-access/64346?camid=4v1a

Applied Cryptography for Security and Privacy in Wireless Sensor Networks
www.igi-global.com/article/applied-cryptography-security-privacy-wireless/37581?camid=4v1a