Security Analysis and Recommendations For MediDoc Inc

CPSC 253

Alejandro Fonseca

Founder, CEO, and Senior Security Consultant for BizSecure

BIZSECURE

MediDoc

Executive Summary:

Medidoc Inc., a fast-growing and expanding healthcare tech company based in Pismo Beach, California faces cybersecurity challenges that could compromise the confidentiality, integrity, and availability of the sensitive patient information that they are tasked of handling. Currently, their cybersecurity posture is inadequate to protect the company from a variety of common cybsersecurity threats. The company lacks redundancy in its systems, transmits data unencrypted, relies on public Wi-Fi and demonstrates many other weaknesses. These practices make MediDoc vulnerable to a variety of cyberattacks, including data breaches, ransomware attacks, and denial-of-service attacks.As the company's Chief Technology Officer, Tom Zeigler, seeks to maintain the organization's clean security record, this report provides an in-depth analysis of potential threats, vulnerabilities, and recommendations to strengthen MediDoc's cybersecurity posture.

Introduction:

With the recent surge in business and the increased use of digital records, securing sensitive patient information is paramount for the continuation of smooth business operations and growth. The company's software is used by a variety of healthcare providers to manage patient records, file insurance claims, and track billing information. MediDoc stores a large amount of sensitive patient data, including names, addresses, dates of birth, and medical histories. As the company has grown, its cybersecurity posture has not kept pace. The company has failed to implement a number of critical security measures, and its existing ones are not well-maintained. This report seeks to examine the company's demographics, services, assets, and infrastructure to identify vulnerabilities and propose effective solutions.

Potential Problems/Threats:

1. *Authentication Server Vulnerabilities:*

The System Administrator is the single point of contact for granting access to company assets. Relying on a single System Administrator as the exclusive point of contact for granting access to company assets poses inherent security and operational risks. This single point of failure introduces dependencies that can lead to delays in access when the administrator is unavailable which could lead to delays or potential oversight. This approach lacks the necessary checks and balances associated with the principle of segregation of duties, thereby raising concerns about accountability and potential conflicts of interest. As the organization grows, scalability issues may arise, with the workload on the System Administrator becoming increasingly challenging to manage efficiently. Additionally, the concentration of access control in one individual raises the concern of insider threats. More importantly, a threat actor now only needs acces to the administrators account to have complete acces versus the need of having acces to multiple accounts to conduct malware attacks, data breaches, and other system manipulation.

2. *Application Server Risks*

Locally hosted databases such as that of SureFile and Quickbooks have a single pointb of storage. Normally, this would not be cause for great concern but since MediDoc has a lack of redundancy and backups, if there is a hardware failure, data corruption, or malware attack, there is a high risk and possibility that patient and financial data may be lost permanently. This can lead to at the minmun a loss of consumer confidence and at most loss of critical data which could put the future of the company in serious jeopardy. Additionally, SureFile which contains PII (Personally identifiable information) is accessible with login credentials regardless of network access. The absence of network restrictions means that the application can be accessed from any network, potentially exposing it to unauthorized access from insecure or compromised networks.

3. *Public Wifi and Work from Home (Employee Devices Risks)*

A good portion of the MediDoc staff relies on public Wi-Fi networks, exposing their devices to a substantial amount of potential cybersecurity threats. Public Wi-Fi networks, such as those found in coffee shops, airports, or hotels, are often less secure than private networks. Additionally, the lack of endpoint protection (such as antivirus software, firewalls, and intrusion detection systems) on these devices increases the risk of malware infections. This can expose the employees to Man-in-the-Middle Attacks where a malicious actor intercepts and potentially alters the communication between two parties without their knowledge. This can lead to unauthorized access to sensitive data, including login credentials and confidential information. Additionally, data Interception can be a big issue as without the protection of secure channels, data transmitted over public Wi-Fi is susceptible to interception. This interception could lead to the compromise of SPI or other confidential data. Without the use of VPNs and the continued practice of allowing employees to use unsecured networks which can also include their home network, MediDoc's security posture is at great risk.

4. *Unsecured/Unencrypted Patient Document Transmission*

Customers such as physicians, dentists, and other hospital routinely send unencrypted patient documents via email or upload them to cloud storage platforms like Dropbox. This practice introduces a significant security concern as the lack of encryption exposes patient documents to the risk of unauthorized access during transmission. Without encryption, sensitive patient information is susceptible to interception by malicious actors or unauthorized parties. The threat actors are easily able to see the data and collect it since encryption wouldn't be hiding the info even if it was intercepted. This can lead to eavesdropping on email communications or unauthorized access to cloud-stored documents and put the company at serious risk or even out of business if the customers no longer trust MediDoc to keep their patients SPI secure.

5. *Lack of mitigation and Recovery Plans*

MediDoc currently lacks a structured and documented approach for dealing with security breaches. In the absence of a comprehensive incident response plan, the organization is vulnerable to prolonged downtime and data loss in the event of a cybersecurity incident. The absence of a well-defined incident response plan poses a significant threat to the organization's ability to respond effectively to cyber incidents and puts the company in a postion where there is no gameplan to stop or contain a malware attack/data breach. This can lead to extended periods of system unavailability, compromised data integrity, and potential reputational damage at the minmun. It is not uncommon for companies in a similar security posture situation completely implode based on reputation after the attack and financial losses resulting from the attack.

Recommendations/Follow-Up Actions:

1. *Implement Robust Access Controls & Secure Application Servers*

To address the vulnerabilities in the authentication server, implementing regular backups, off-site redundancy, and introducing multi-factor authentication (MFA) will significantly enhance access control and reduce the risk of unauthorized access. Additionally, it would be good practice to have more than one point of authorization by a single administrator. Having a sepration of duties and practicing least privilege will significantly improve MediDoc’s security posture. Moreover, by establishing regular automated backups, introducing network access controls, and encrypting sensitive data, the security of both SureFile and Quickbooks can be significantly improved, reducing the risk of data loss and unauthorized access.

2. Secure Employee Mobile Devices

Enforcing the use of virtual private networks (VPNs) and deploying endpoint protection software on all mobile devices will mitigate the risks associated with sales staff using public Wi-Fi, reducing the likelihood of malware infections and data breaches. Additionally, it may be wise to advise staff to minimize the use of public wifi and reduce the prominence of the work-from-home structure.

3. Secure Patient Document Transmission

Implementing end-to-end encryption for patient documents during transmission like hashing and salt while also educating customers on secure submission methods will enhance the confidentiality and integrity of patient information. This can be done by using secure file transfer software instead of a basic commercial one like Dropbox.

4. Develop and Implement Incident Response Plans

Creating and implementing incident response plans, including communication protocols and recovery procedures, will ensure a swift and effective response to any security incidents, minimizing potential downtime and data loss. This is a non-negotiable and a baseline requirement to have a passable security-posture. No matter what precautions you take, the possibility of a cyber attack is always there and having a good incident response plan will put you in the best position to respond.

Conclusion:

This report underscores the critical need for proactive measures to fortify MediDoc Inc.'s digital infrastructure. The vulnerabilities identified pose potential and significant threats to patient data and overall business operations. The recommendations, ranging from robust access controls and secure server practices to incident response planning, collectively provide a strategic roadmap for strengthening the organization's cybersecurity defenses. Embracing these measures not only safeguards sensitive information but also aligns with the commitment to maintaining customer trust. As the company navigates its rapid growth, the proposed actions serve as a foundation for a resilient cybersecurity framework.

References:

1. Stallings, William. *Computer Security: Principles and Practice*, 4th ed., Publisher, Year of Publication.

2. National Institute of Standards and Technology (NIST). "Digital Identity Guidelines: Authentication and Lifecycle Management." NIST, 2017.

3. Center for Internet Security (CIS). "CIS Controls Implementation Guide for Small-and Medium-Sized Enterprises." CIS, 2021.

4. International Organization for Standardization (ISO). "ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements." ISO, 2013.