Interviewing CTO Tom Zeigler related to cyber security concerns for the company Medidoc

By Kush Patel
CPSC 253
Jason Choi

Hello, My Name, is Kush Patel, I am a Senior security consultant for BizSecure, an up-and-coming security firm that offers consultancy services for businesses, I am responsible for offering a service that includes a security analysis of the business, the client I am interviewing is mediocre, and I have interviewed the Chief Technology Office about the current state of MediDoc Inc, such as it's demographics, which include people from different sectors such as Executives, Salespeople, Accounting, and the Information Technology Department. Some people in different sectors have to work on-site such as the IT Specialists, in which we are going to address problems and concerns related to cyber security and IT Specialists in MediDoc Inc. What I hope that the people who are reading my report is that they understand all the problems relating to the company information security and systems and suggestions they will take from me.I plan on addressing the concerns and problems related to technical security and other problems with MediDoc, by providing as many solutions and changes to their technologies as much as possible.I also gathered information on what devices the company use, and what type of networks the company uses. We provide so many services such as an identity provider that manages customers. There is a lack of human resources for contacting to grant access to company assets, which are a huge and important factor that is related to cyber security. To explain the problem of fewer human resources to grant access to the assets, the only way to get access to the company's assets includes an authentication server, application server, and servers, which you have to contact the system administrator directly. This isn't a good thing, because what if he's not there, he's sick, he's in the hospital, or any unforeseen consequence occurs, then a way to address the lack of human resources issue is to provide security training, awareness, and education to more people and provide people to more of these opportunities, and by providing these training programs to more employees and people, it improves the employee's behavior, increases their accountability, it mitigates liability for their behaviors, and they comply with regulations. Doing all four of these things, not only addresses a major concern, but also minor concerns such as the lack of responsibility, less motivation, and not being cautious at all. The more people who are trained and trusted with providing access to assets to other people, the more safe and secure these assets are, because these people after they are trained will learn to provide stricter background checks to people who are trying to access these assets, which prevents phishing and cyber-attacks within their company. The stricter the background check these people provide, the less likely cyber crimes will occur, in which MediDoc inc, is a huge target for cybercrimes, due to the lack of background checks and security, which is a huge concern for this company. This company should include more background checks equally for everyone rather than just one sector of people because if they do it just for the IT department then there will be so many consequences and make the company more vulnerable to cyber-attacks. With the company being a huge target for cyber crimes, there is a high chance that SQL injection attacks could occur. Due to the lack of training and knowledge of how to do defensive coding when trying to prevent SQLi injection attacks, this company has also become a victim of SQLi injection attacks. Due to the lack of training programs that these employees don't get, they are based on a Role-Based Access form. With also the lack of training problems they also have a higher chance of becoming victims of SQL injection attacks, where their data could be erased or modified, which can lead to so many huge consequences for the company, in which they can’t find out what problems there are and many people in the company could lose their jobs.There is a Role-Based Access form when accessing assets within this company because in order to grant access to the asset in this company, you will have to contact a specific person with a given role which was The System administrator. The drawback of having a Role-Based Access Control form is that there are temporary setups, in which only the System Administrator does the work, and if he or she is gone or not there, there would be a hard time gathering information. There is also a labor-intensive setup that requires so much time and work to the point where the attacker would have plenty of time to attack. Another concern this company has is that its’ customers which are health care professionals send unencrypted messages which are the people's medical documents sent through email. Here are so many downsides to sending medical documents and other messages that are unencrypted. Unencrypted messages can provide attackers with a broader field of what to attack when they receive those medical documents. There will be a larger attack on the company when the attacker does it which would lead to so many people being laid off and losing their jobs. We must provide comprehensive protection whenever we send out an email. The emails that are sent are at risk. The risk is that it can get lost or stolen by a third party, and they can get unauthorized access, which can cause your data to be modified and stolen, and when your data gets modified or stolen, it can lead to huge consequences on that person including fraud and identity theft, a way to prevent this is to unencrypt the message or make sure to have the person you want to show the data meet with you in person or virtually. By encrypting all messages we are adding an extra layer of protection to sending messages and our business and causing fewer worries within the business. If we encrypt more data in the email or the entire message itself less people will have access to attacking the servers, which would lower the chances of having any data modified within the email or any messages. The data that is not encrypted is considered unprotected sensitive data. Having unprotected sensitive data can lead to identity theft of customers and employees, fraud, and theft of the financial resources within the company. When someone's identity is lost, they could have all their money stolen, they could lose their job, or they could have a bad reputation until they find out who was the cause of the identity theft. Whenever accused of fraud, they could be falsely arrested and lose their job which happens to a lot of people. When there is a theft of financial resources of the company employees and customers, not only do the customers and employees lose all their money and insurance, but they also lose all the assets of the company including authentication and application servers which are very important for the company, because it protects the company from so many dangers, and by sending unencrypted messages, it makes the company more vulnerable to phishing or any other cyber attack. The company should send encrypted messages because it protects the privacy of the company, the employees within the company, and its customers. There is also an integrity of data if all the messages are encrypted within the company, in which the attackers don't have the key and password to access data and the customer data is protected from outside viewers who are not the customers. When we do end-to-end encryption within a company, the company should do that to prevent unauthorized devices from opening any of the messages that are sent. By only allowing authorized devices to open any messages, it keeps them safe from any attacks or any unauthorized person from deceiving the person who is sending the message to them. Whenever an attacker gets the message accidentally, it would be hard for them to decipher and try to encrypt the message themselves. Whenever a hacker tries to overcome end-to-end encryption, they will fail by doing the most difficult and time-consuming device hack they would try, which causes most hackers to quit and give up that approach. The company should include end-to-end encryption which is considered one of the main problems they have and to address their concern they should hire more cybersecurity professionals who have so many years of experience to implement those safety features. They plan to avoid High-Cost Attacks, which would lead to all their employee's and customers' accounts being inaccessible and would cause them to have a bad reputation. The employees must be very careful when sending out messages because attackers can easily get their messages. Another problem and concern for this company are that the employees rely on public wifi, which can be unsafe and dangerous similar to when you use online banking on public wifi. Using public wifi can expose your computer or any other device to viruses and other cyber attacks which can cause all your data to be modified or erased. It can allow hackers to use malware to inject into your device. The company should switch and create its own private wifi network. A person doesn’t know how a public wifi network was set up.People should avoid public wifi as much as possible, but they should try to stay safe from it by following so many mitigation measures by not paying any bills, not doing anything financially related, don’t do any social security stuff, if they ever want to use public wifi or public wifi is their only option, they should avoid using sensitive information, they should use a VPN, they should use websites that have SSL certificates, to identify a website with an SSL certificate or if it is secure, the website URL should start with “https", in which the s in “https” means it’s secure, they also set up two-factor authentication in their websites. To address their problem and concern about using public wifi they should set up their own private wifi network, to which only the company and its employees are able to do stuff, see things, and access it. They should set up their own private wifi network by creating so more of a mind map or diagram to keep an eye on all the devices that are connected to the network and make sure they are familiar with those devices, they should also create their own firewalls to control incoming and outgoing traffic within their network. Employees are better off coordinating an asymmetric encryption model with a public/private key because it is safer and more manageable to share a public key with the senders. They can allow certain traffic and block any unfamiliar traffic that is not related to them. Despite antiviruses not being fully effective they should include them in their firewalls and other software for extra protection or to slow down any attacks from viruses. They should also create an address plan for their networks because they must include a unique IP address that only certain devices should know about that way it can prevent any computer viruses from getting into their private network. They also should assign specific devices to a specific network because if they have a device that they don’t trust or not very well, there will be a very high chance for that device to have an attacker attack their services.They should create specific devices that keep their routers safe. They also should choose a network host range in which only certain devices can gain access to the networks and can mitigate and minimize traffic. Implementing all of these things into the company, lessens the concerns about the network the employees are using, and by doing all of these mitigations we will decrease the likelihood of another cyber attack from happening to the company or any viruses infiltrating the servers of the company. The employees should stop using public wifi everywhere or else they'll get into so much trouble with all of their networks and other systems within their companies from loss of data to identity theft. Medidoc is a huge target for cybercrimes such as SQLi attacks, viruses, and Denial of Service Attacks. To prevent all of that from happening the company could install intrusion prevention and detection systems, and they should install addresses that prevent the attackers from modifying their credentials. They also should implement proper defensive coding practices. Implementing defensive coding practices is to contract to design the algorithms and they should program and algorithm assertively.They also should implement algorithms in the systems which it would prevent an attacker from even trying to access the webpage or even turning on the device, one way is to do is to put a fingerprint identity verification on a device to see if that person who wants to turn on that device has the right to do so, if they don't then the device doesn't turn on. They also should create a Host-based Intrusion Detection System because it directly protects at the endpoint.The Host-Based Intrusion System also blocks malicious actions before they have a chance to modify any of the systems. By also implementing Host-Based Intrusion Detection systems it adds a specialized layer of security to any weakened and vulnerable security systems. They also send alerts immediately as soon as there has been a cyber attack. A way to defend against SQL injection attacks is to validate the input a person gives when a person is giving his or her information, by issuing a two-factor authentication. They can also implement parameterized queries where professionals of the business/company can write specific statements in the line of code to provide warnings in advance and prepare for any uncertainties. They should ask directly for input. You should always read through the input clearly by issuing a two-factor authentication.We also ask specific security questions only the user should know. We should ask them for their face or voice id because nobody knows what a cyber criminal looks like because their face and voice aren't seen or heard. They should also sanitize their input in every different way or form as much as possible. They should also implement vulnerability scanners. They should also implement a prepared statement variable to provide a defense to the code. They should also do code analyses and anomaly detections to achieve defensive coding. They should also implement run-time prevention, where they can check the queries to show they can prove they're not attacked. They also should utilize cloud services because it can create huge benefits for their security. They should also make sure that downloads are not modified during the download by verifying a provided hash of the downloaded software. They should also include Software as a Service because it is more convenient, it is messy to maintain, and it has better usability. Out of the Hybrid, Host-Based, and Network-Based Intrusion detection systems, the best one to use when protecting against any cybercrime is Hybrid because it is more secure than the other three. They should always hash and store passwords. They should implement either Signature, Heuristic, or Anomaly detection approaches for Intrusion Detection and Prevention Systems, because all three can equally detect more traffic quickly and suddenly increase compared to the other type of detection approaches. They shouldn’t look for queries for a true/false answer to the database and based on the response gets what it needs, because it can lead to blind SQLi attacks. If they want to protect the assets on the employees' laptops they should implement a Host-Based. They should also try to get as many SSL certificates as possible when creating their own websites because it not only keeps their websites safe but also other people when they try to access their websites. Another problem and concern I want to address for this company are that there is no mitigation or recovery plan. The lack of a mitigation or recovery plan during failures, breaches, or any other situation can lead to so many consequences. It is important to have a mitigation plan because it reduces the likelihood of a cyber attack, which hasn’t happened to this company yet, but let's hope it doesn’t happen and that we can create a mitigation plan for them. It’s a good decision-making process around risk control and it keeps your organization protected from more attacks and achieves all of its business goals. If the company implements mitigation measures, it must have an uninterruptible power supply for each critical piece of equipment. They must restrict building access, they must guard controlled areas, must have screening measures at entry points. They must equip movable devices or other resources with a homing beacon or some other tracking device, they must have intruder sensors or alarms. To implement a mitigation plan which they should’ve, they should have daily risk assessments, establish network access controls, continuously monitor network traffic, they must create an incident response plan, should continuously update software, and we must increase our hardware security systems. They should also establish the owners of specific devices and systems within the company. They also should set up disaster recovery sites. They also should implement data backup protocols. The company's lack of a recovery plan could also lead to data being lost or modified within their company and by having a recovery plan, they get a roadmap on how they can disrupt more cyber attacks such as data breaches or ransomware attacks which could lead to loss of data. After talking about all the problems, explaining the results and effects of what those problems have on the company, and how we solve and prevent those problems from happening in order to feel less concerned about the company’s security and keep the company safe from any cyber attacks, I hope this company implements all my suggestions and succeeds in the future. Cyber Attacks are easily preventable if a company or a single person follows specific guidelines on making technology safe, using technology wisely, and taking extra precautions when using precautions.

References

"What Is RBAC? (Role Based Access Control)." *IONOS Digital Guide*, https://www.ionos.com/digitalguide/server/security/what-is-role-based-access-control-rbac/#:~:text=Advantages%20and%20disadvantages%20of%20RBAC,-In%20some%20cases&text=Any%20modifications%20to%20the%20organizational,of%20individually%20assigning%20permissions%20obsolete.

AG, Brainloop. "Three Reasons Not to Use Email Encryption - Brainloop - UK." *Brainloop*, 23 Mar. 2022, https://www.brainloop.com/en-gb/three-reasons-not-to-use-email-encryption/#:~:text=Unencrypted%20emails%20provide%20criminals%20with,or%20read%20the%20unencrypted%20text.

"Encryption Scenarios." *ICO*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/encryption/encryption-scenarios/#:~:text=If%20you%20send%20the%20data,an%20additional%20layer%20of%20protection.

Hiter, Shelby. "End-to-End Encryption: Important Pros and Cons." *CIO Insight*, 15 Feb. 2023, https://www.cioinsight.com/security/end-to-end-encryption/.

Stouffer, Written by Clare. "Public Wi-Fi: An Ultimate Guide on the Risks + How to Stay Safe." *Norton*, https://us.norton.com/blog/privacy/public-wifi#:~:text=Yes%2C%20a%20public%20Wi%2DFi,device%20with%20viruses%20and%20malware.

wikiHow. "How to Set up a Private Network: 11 Steps (with Pictures)." *WikiHow*, WikiHow, 11 Oct. 2020, https://www.wikihow.com/Set-up-a-Private-Network.