Daniel Weinert
CSS-2753
3/14/2021

Strategic Hospital Information Security Roadmap

This security roadmap, which will be presented to the board of directors, outlines all the steps necessary for the information security department to ensure that all hospital systems are operating at full capacity with no downtime and are adequately protected. Also addressed in this report will the recent successful phishing scams against many of the hospital's employee and the action plan to curve the successfulness of these attacks. Lastly, we will go over the new policies regarding healthcare and personal data on our computer systems.

According to recent security reports we have seen a spike in successful phishing attacks against our hospital. Due to this we are creating new policies and actions to combat these phishing attempts. First, we will build a brand-new training program to help employees understand what a phishing attempt is and how to spot it so that you do not fall victim to it. After everyone has successfully completed the new phishing training, we will implement a quarterly phishing exercise. For this we will use the tool PhishMe by CoFense which will send out dummy phishing attacks to our employees. If an employee fails the exercise and clicks on the link in the email they will automatically be added to a follow up phishing training. On top of that we will purchase the Web Security Service package by Symantec which will filter and scan emails and other communications for phishing attempts so that they can be intercepted and stopped before ever reaching an employee.

Regarding the two recent breach attempts against our system, we have overhauled our policies regarding access control, encryption and authentication. We discovered holes in our previous policies and way of doing things that allowed for certain points of entry to not have adequate security and certain system had almost no protection. Along side these changes we will implement a new firewall system by PaloAlto because our old firewalls have become outdated since they were bought years ago as a single software and not a subscription package with security and improvement of life updates which we will now receive. The new web security package which was mentioned in the previous paragraph will also help out by monitoring and protecting all web related connections. This system with the new firewall will also make sure that we can reduce the risk of DDOS attacks against our systems. So far, we only really had one major attempt at such an attack but should now be better prepared. If these systems don’t seem to protect us from DDOS attacks we will look at systems like DDOS protection by Cloudflare but we don’t believe we have reached a level where this is necessary yet. We are also currently working with HR and the finance department to create a report which will outline the costs related to an outage of our systems.

Our last challenge in this roadmap is to ensure we have a good overview of where we store HIPPA and Pii related data, who has access to it and to make sure it is adequately protected. For the first challenge we have already began to schedule interviews and sent questionnaires to all department heads asking what type of data they use, process and if they store it, where. Once we have completed this phase of information gathering, we will write a report which will lay out all the departments use of data so we have an overview of how data is used and stored throughout the hospital. Once that is done our first primary focus will be to ensure that at no point any piece of data is stored unprotected and that the way of storage works correctly for each department, once that is ensured we will move on to transfer and make sure that at no point is data unencrypted while in transfer either inside the hospital or to an outside source like a vendor. Once this groundwork is completed, we will hire an outside firm to perform a HIPPA, Pii, (and any other data law we may fall under) audit to ensure we follow all laws and regulations and to get a second set of eyes on our system to ensure everything is done the best way it could be.

To wrap this security outline up we will overview the major points. First, we outlined how we are going to bring down the successful phishing attacks against our company by implementing new trainings and software solutions. Then we discussed the major breach attempts against our system and how we will ensure that they will remain unsuccessful attempts. Then lastly, we covered how we will govern data from now on regarding usage, transfer and storage. This roadmap will only require a small budget for the new software solutions nowhere near as much a potential outage could cost us and the rest only requires internal work within the organization that just costs time and manpower.

References:

CoFense. “Phishing Awareness Training & Tools: Phishing Simulations.” *Cofense*, 3 Feb. 2021, https://cofense.com/product-services/phishme/

Gerber, Scott. “11 Security Strategies to Protect Your Company from Phishing Attacks.” *The Next Web*, 16 Mar. 2018, https://thenextweb.com/contributors/2018/03/23/11-security-strategies-protect-company-phishing-attacks/?utm_source=copypaste&utm_medium=referral&utm_content=11+security+strategies+to+protect+your+company+from+phishing+attacks&utm_campaign=share%2Bbutton

Symantec WSS. “{{SeoKeywords}}.” *Help.symantec.com*, https://help.symantec.com/cs/ccd/CCD/v132149022_v129301524/Symantec-Web-Security-Service-(WSS)-integration-FAQs?locale=EN_US

Yitoh. “Azure DDoS Protection Standard Overview.” *Azure DDoS Protection Standard Overview | Microsoft Docs*, https://docs.microsoft.com/en-us/azure/ddos-protection/ddos-protection-overview