Meeting minutes- 11/15/2024

Group leader of the week: Tobey Chan

Meeting summary (11/12/2024 at 6:00 pm) our group called in together over discord to discuss this week's progress in research and how we are going to implement the information into our presentation.

Present members: Sohaib Chachar, Tobey Chan, Ranique Huggins, John Nasseh

Meeting agenda:

- seeing where everyone's progress is in regards to last week's assigned research material
- Establishing what the following weeks will look like for progression:
    1. week 3 putting together research into completed slides
    2. Week 4 taking completed slides practicing the presentation in person with one another

Notes: John, Ranique, and I (Tobey) while having done research and have started the process of getting information down in writing have not finished the full write up yet. Sohaib is finished currently with his research and write up and is now in process of collaborating with Ranique to help match all of their talking points within the solutions portion of the presentation. We are mainly using this meeting to catch one another up on our progress and to plan accordingly for the rest of the week.

(Tobey Chan) State of current threats

Primary issues and the current state of threats to hospitals:
One of the main consistent forms of cyberattacks targeted at hospitals is ransomware which is a type of cyber attack that takes control/denies access to important files/systems and relinquishes back access to these systems after an exchange of payment. This type of attack, while being a major concern for security and confidentiality, is also a major concern in regards to life and death within the context of ransomware attacks on hospitals. As these institutions are responsible for keeping the injured, sick, and old alive and healthy, the threats of denied access to important systems within these hospitals could mean a patient's chances of surviving their stay in critical condition lowers.

As quoted here from the source, UN news article, "*Cyberattacks on healthcare: A global threat that can't be ignored*"

"At best, these attacks cause disruption and financial loss. At worst, they undermine trust in the health systems on which people depend, and even cause patient harm and death."

Some aspects of ransomware becoming more of a prominent threat to hospitals is the observation that cyber criminals that frequently attack hospitals using this form of cyber attack, not only target the hospital's systems but are also capable of targeting specific medical equipment. Ransomware is no longer being carried out by amateurs but by experienced hackers and mercenaries with some form of foreign backing/protection. These cyber attacks being aimed at health facilities has only aided in increasing the success rate of ransomware attacks. Hospitals can't afford to deny these attackers, and criminals know this as well. As mentioned earlier lives are at stake.

References

"Ransomware Attacks on Hospitals Have Changed: Cybersecurity: Center: AHA." ***American Hospital Association*****, www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed. Accessed 15 Nov. 2024.**

"Cyberattacks on Healthcare: A Global Threat That Can't Be Ignored | UN News." ***United Nations*****, United Nations, news.un.org/en/story/2024/11/1156751. Accessed 15 Nov. 2024.**

(John Nasseh**) Modes of attack**

Hospital Cybersecurity Modes of Attack
1) Ransomware: malware that encrypts hospital data, blocking access until a ransom is paid. This can cripple hospitals by rendering medical records and systems inaccessible, forcing staff to resort to manual processes and sometimes even shutting down critical services.
2) Phishing: phishing attacks trick employees into giving up sensitive information or downloading malware through deceptive emails. This can lead to unauthorized access to patient records, financial info, and hospital networks. Hospitals are very vulnerable to phishing attempts due to how many employees they have.
3) DDoS attacks: overwhelm hospital networks with traffic, causing system slowdowns or crashes. It can disrupt critical functions such as patient record access or appointment scheduling. Telemedicine services, etc
4) Supply chain attacks: Hospitals rely on third-party vendors for various services, including IT management, medical devices, and software. If the vendors have weak security practices, attackers can exploit them to access the hospital's system.
5) Data breaches: hackers may target electronic health records to steal sensitive patient info, which can be resold. This can also lead to significant legal and financial repercussions for the hospital
6) Internet of medical things (IoMT) vulnerabilities: Hospitals use internet-connected medical devices. These devices often lack robust security protections and can be vulnerable to attacks that disrupt their functionality.

(Sohaib Chachar) Solutions

Defensive Strategies Against Ransomware Attacks

Advanced Backup and Recovery Solutions

If you want to lessen the damage that malware does, you must keep full and safe backups. Ransomware can lock or remove backup files, so simple backup methods aren't always enough to keep you safe. They came up with new ideas, such as the content-based ransomware detection and backup solid-state drive (SSD) that can find ransomware in real time and get your data back right away. This SSD architecture tracks how data is viewed and looks for ransomware activities based on the content of the data. This makes it easy to quickly recover files that were damaged from safe backups, which cuts down on data loss and downtime.

Network Segmentation

By separating a network into separate sections, ransomware can't move from one part of an organization to another. By limiting access between network zones, hospitals can keep

infections in certain places, which lowers the damage that could happen. As Divakaran and Oest (2022) say, this approach stops ransomware from spreading and keeps important systems and private data safe.

Endpoint Detection and Response (EDR) Systems

Using EDR solutions lets you keep an eye on endpoints all the time so you can quickly spot and stop any strange activity. These systems can spot strange behavior that could be a sign of ransomware attacks. This lets you quickly find and fix threats before they do a lot of damage. EDR tools let you see what's happening at endpoints in real time, which makes it easier to find threats and handle incidents (Divakaran and Oest 2022).

Regular Software Updates and Patch Management

To protect yourself from ransomware, it's important to make sure that all of your software and systems have the latest security changes. Ransomware is often spread by cybercriminals using known flaws in old software. This kind of organized patch management helps close these security holes, making it harder for attackers to get in (Shahrivari, Darabi, and Izadi 2020).

Defensive Strategies Against Phishing and Spear-Phishing Attacks

Employee Training and Awareness Programs

Cybersecurity shortcomings are often caused by things that people do. It's very important that employees get regular training on how to spot phishing efforts. A study by Jampen et al. (2020) proved that teaching people about security does make them less likely to fall for fake attacks. Giving comments on fake phishing exercises is one way for healthcare centers to help their employees spot and report phishing emails. The company is safer generally because of this.

Big Data Analytics for Phishing Detection

It is possible to use big data analytics to look through big records for phishing trends and other strange things. A study by Shahrivari, Darabi, and Izadi (2020) looked at how machine learning can be used to find fake websites by looking at a lot of different aspects of websites. Their work shows how big data analytics can be used to make it easier to find phishing sites. This can help make models that can find phishing sites correctly. Phishing efforts can be found and stopped before they reach end users with this kind of information.

Email Filtering and Anti-Phishing Technologies

Smart email blocking tools can help find and block phishing emails before they reach employees' inboxes. There are technologies that look at emails, the sender's image, and other things to see if they might be attempts to phish. Adding anti-phishing tools that warn you right away about files or links that might be dangerous makes security even better (Jampen et al. 2020).

Multi-Factor Authentication (MFA)

MFA makes systems and data safer by requiring users to prove their identity in more than one way before they can access them. MFA can keep people from getting in without permission, even if passwords are stolen through phishing. This keeps private data safe. This way makes it much less likely that phishing attacks will be successful at taking over your account (Shahrivari, Darabi, and Izadi 2020).

Regular Security Assessments and Penetration Testing

Regularly checking and keeping an eye on your security can help you find holes that hackers could use. These reviews show how well the security methods we have now work and where they could be improved. If healthcare centers find and fix any flaws, they can make their defenses better against phishing attacks (Jampen et al. 2020).

References

Divakaran, Dinil Mon, and Adam Oest. 2022. “Phishing Detection Leveraging Machine Learning and Deep Learning: A Review.” *arXiv (Cornell University)*, January. doi:10.48550/arxiv.2205.07411.

Jampen, Daniel, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. 2020. “Don’t Click: Towards an Effective Anti-Phishing Training. A Comparative Literature Review.” *Human-Centric Computing and Information Sciences* 10 (1). doi:10.1186/s13673-020-00237-7.

Shahrivari, Vahid, Mohammad Mahdi Darabi, and Mohammad Izadi. 2020. “Phishing Detection Using Machine Learning Techniques.” *arXiv (Cornell University)*, January. doi:10.48550/arxiv.2009.11116.

The increase in the incorporation of technology into healthcare has led to greater precision in patient care, however this also comes with increased security threats. Key threats to a large hospital system today include phishing attacks, insider threats and vulnerabilities in medical devices. To combat this requires a multi-layered approach to adequately secure the healthcare facility from cyberthreats. The main concern of healthcare systems is to prioritize the protection of highly sensitive patient data, adhering to HIPAA regulations.

(Ranique Huggins) More solutions

The Recommendations are as follows:

- **Strong Identity and Access Management (IAM) by Strengthening Access Controls**

There are great risks associated with granting administrative privileges to users in healthcare facilities. Organizations should implement multi-factor authentication, have regular access reviews, role-based access control and strict password policies to reduce unauthorized access risks. They should also encrypt sensitive data both in transit and at rest to protect it even if it is accessed without authorization. An investment in advanced threat detection would also prove beneficial as the use of artificial intelligence and machine learning to detect abnormal network activity can help to mitigate risks

· **Employee Security Awareness Training:**

Humans are the weakest link in cybersecurity therefore, it's necessary to regularly educate staff on phishing detection, password hygiene, and safe online practices. To offer relevant and effective training, health facilities should frequently assess and identify gaps in knowledge.

· **Vulnerability Management:**

In order to expose the vulnerabilities, the hospital should regularly scan for and patch software vulnerabilities across all systems, including medical devices. The organization should maintain this practice for early detection can help reduce exposure to security risk. Patching should be applied to all systems, even the third- party applications.

· **Incident Response and Disaster Recovery Plans:**

Cyberattacks have occurred more frequently in recent years and health facilities should be well equipped with an incident response and recovery plan. Intrusion detection and prevention systems (IDPS) can help in spotting threats early. The organization should develop a comprehensive plan to detect, contain, and remediate cyber incidents efficiently. They should develop and routinely test a comprehensive response plan for ransomware and other cyber incidents, including backup strategies to restore critical data without having to pay ransoms to criminals. These plans should be regularly tested and stored offline with clear post- incident steps.

· **Cybersecurity Insurance and Collaboration with Regulatory Bodies:**

The organization should also consider obtaining insurance coverage to mitigate financial losses from cyber incidents. It is also in the organization's best interest to stay informed about the evolving cybersecurity regulations and the recommended best practices. By actively monitoring the cyberthreat landscape, implementing robust security controls and maintaining a culture of cybersecurity awareness; healthcare systems can significantly limit the risks associated with cyberthreats and protect sensitive patient information.

REFERENCES

· Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D. *et al.* Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC Med Inform Decis Mak* 20, 146 (2020). https://doi.org/10.1186/s12911-020-01161-7

· Mandiant. 2024. Bavi Sadayappan, Zach Riddle, Jordan Nuce, Joshua Shilko, Jeremy Kennelly. "Ransomware Rebounds: Extortion Threat Surges in 2023, Attackers Rely on Publicly Available and Legitimate Tools.

· ZDNET. 2021. Liam Tung. "This is how long hackers will hide in your network before deploying ransomware or being spotted."