CSI4139

Assignment 1

Name: NamChi Nguyen
Student #: 7236760

SingHealth Cyberattack

Background

Near the end of June to the beginning of July 2018, the database of Singapore's healthcare institution SingHealth was attacked. SingHealth used the Sunrise Clinical Manager (SCM) software by Allscripts Healthcare Solutions which was handled by the IT agency for the healthcare sector called Integrated Health Information Systems (IHiS) [1]. SCM originally ran on Citrix servers accommodated by Singapore General Hospital (SGH) but then in July 2017, the database and servers were migrated to a private cloud called Healthcare-Cloud (H-Cloud) that was used by Singapore's regional health systems [2], [3].

The Attack

The attack was discovered by IHiS database administrators after observing abnormal activity in SingHealth's IT databases. The attacker had gained access to the system through a breach on a front-end workstation after obtaining Citrix admin credentials to log into the Citrix server. The vulnerability that was exploited was that after the migration to the cloud, an open network connection between the Citrix sever hosted by SGH and the SCM database server on H-Cloud still remained. Furthermore, the open network connection was used to run a vast amount of bulk SQL queries between the Citrix server and SCM database server. Also, one of the local database administrators had a weak password called P@ssw0rd [1], [4], [5].

The Cyber Security Agency of Singapore (CSA) and IHiS determined that the cyberattack was thoroughly planned and was later revealed at the Committee of Inquiry's (COI) public hearing that the cyberattack displayed qualities of an advanced persistent threat (APT) attack in which the attacker(s) made persistent attempts to access the data by using advanced hacking tools and personalized malware that bypassed antivirus software [1], [4], [5].

Repercussions of the Attack

The damage was severe, as the personal information of Singapore's prime minister Lee Hsein Loong along with approximately 1.5 million patients were stolen and copied between June 27 to July 4, 2018. These were patients who had visited outpatient clinics and polyclinics between May 1, 2015 to July 4, 2018. The personal data included names, NRIC numbers, addresses, genders, races and birthdays but excluded telephone numbers, passwords and credit card information. Additionally, the outpatient dispensed medicines of 160 000 patients were also accessed but none of the patient and database records were altered [4], [5].

The unauthorized queries were terminated by IHiS database administrator Katherine Tan on July 4th and no further data exfiltration continued afterwards. However, despite ending the attack, the IHiS staff didn't alert the senior management until July 9th and by July 10th, SingHealth, Ministry of Health and CSA were notified and then became known to the public on July 20th [1].

Recovery and Procedures

To recover as soon as possible from the breach, IHiS and CSA enforced a temporary internet surfing separation, reset the user and system accounts and appointed more system monitoring controls. All patients were gradually contacted even if they weren't affected through SMS notifications after the news was released to the public. Patients could also verify if their data had been compromised through a mobile app or the SingHealth website [4].

Thus, SingHealth's main action to recuperate from the breach was by internet surfing separation (ISS) or also known as network separation/air-gapping. It is "the practice of isolating computers used by staff, which are connected to an internal network, from establishing a connection to the internet" [6]. By this method, it was considered more secure to stop the continuation of the cyberattack since the attacker would not be able to access the data offline. Although, ISS would reduce the productivity of the staff as some systems would require internet access and implementing this practice would be expensive long-term. Lastly, despite the computers being offline, if the attack was from within the company, complete protection wouldn't be guaranteed [6].

A possible action that the IHiS database administrators of the system could have taken to minimize the impact of the cyberattack would have been to tell the senior management as soon as possible after terminating the bulk SQL queries instead of waiting five days. It wouldn't have costed the administrators to have notified their superiors as the attack had already occurred and further investigations to confirm if it was a threat caused a delay in taking preventative measures immediately.

Also, after discovering that one of the local admin accounts contained a weak password, another suggestion to strengthen the security would be to reassure that all the IT staff were properly trained on creating strong and difficult passwords. In addition, the usage of a strong hashing algorithm for passwords along with salting and password aging to compel staff to change their passwords every x months.

In addition, since internet surfing separation was chosen as a temporary solution, according to Gan Kim Yong who is the Minister of Health, suggested the usage of piloting a virtual browser and utilizing Advanced Threat Protection (ATP). A virtual browser would permit users to securely access the internet through isolated servers [5]. A virtual browser "is a Web browser that is logically or physically isolated from a computer's underlying operating system" [7]. It can be implemented by a virtual machine or a virtual browser appliance which may not be initially feasible as training on how to navigate between the host OS and the virtual machine would be required [8].

Conclusion

To summarize, the data of about 1.5 million patients stored in SingHealth's database were stolen in about a span of a week during late June to early July in 2018. The attacker had executed numerous bulk SQL queries after gaining entry onto the server via an open connection between the servers at SGH and H-Cloud. After the attack was successfully terminated, investigations were conducted, patients were notified of the breach and the temporary solution of internet surfing separation was used during the recovery process.

References:

[1] K. Kwang, “COI for SingHealth cyberattack: IT gaps, staff missteps contributed to incident, says Solicitor-General”, Sept 21, 2018, [Online]. Available: https://www.channelnewsasia.com/news/singapore/singhealth-cyberattack-committee-inquiry-staff-hack-10744182. [Accessed Sept. 23, 2018]

[2] IHiS, “H-Cloud”, 2018, [Online]. Available: https://www.ihis.com.sg/Project_Showcase/Healthcare_Systems/Pages/H-Cloud.aspx. [Accessed Sept. 23, 2018]

[3] E. Yu, “SingHealth data breach reveals several 'inadequate' security measures”, Sept 21, 2018, [Online]. Available: https://www.zdnet.com/article/singhealth-data-breach-reveals-several-inadequate-security-measures/. [Accessed Sept. 23, 2018]

[4] Ministry of Health, “Singhealth's IT System Target Of Cyberattack”, July 20, 2018, [Online]. Available: https://www.moh.gov.sg/news-highlights/details/singhealth's-it-system-target-of-cyberattack. [Accessed Sept. 22, 2018]

[5] Ministry of Health, “Cyberattack On Singhealth's IT System”, Aug 6, 2018, [Online]. Available: https://www.moh.gov.sg/news-highlights/details/cyberattack-on-singhealth's-it-system. [Accessed Sept. 22, 2018]

[6] GenX, “Mind the Air Gap: Pros and Cons of Network Separation”, 2018, [Online]. Available: https://www.genx.ca/mind-the-air-gap-pros-and-cons-of-network-separation. [Accessed Sept. 24, 2018]

[7] M. Rouse, “Virtual browser”, Nov 2014, [Online]. Available: https://whatis.techtarget.com/definition/virtual-browser. [Accessed Sept. 24, 2018]

[8] Dell, “Virtual browser”, 2018, [Online]. Available: https://www.dell.com/support/article/ca/en/cabsdt1/sln311997/virtual-browser?lang=en. [Accessed Sept. 24, 2018]