SECURITY BREACHES BASED ON SOFTWARE VULNERABILITIES

Jordon Coady - 20096529

SECURE PROGRAMMING & SCRIPTING

Contents

Criteria of Breach severity

Each of the factors below can be ranked either 1, 2, 3 or 4. The higher the number the more serve the factor. Below are the three factors that I will be using to determine the severity of the breaches discussed in this report.

1. The first key factor in determining the severity of a security breach is the nature of the breach itself. This includes understanding how the breach occurred, the methods used by the attacker, and the extent of the breach.

2. The second key factor is the type of data that was exposed. Different types of data carry different levels of risk, and some information, such as financial information, social security numbers, or medical records, can have serious consequences if compromised.

3. The last factor I will use to access the severity of the breach is how the company affected respond to the breach. If the company lied about the extent of the data exposed in breach or if the fixes for the exploits were slow to be deployed that would increase the severity of breach.

After assessing the factors in the context of the breaches I will total the score from each factor for an overall rank. 0 – 3 low severity, 4 – 7 moderate severity, 8 – 12 high severity.

Optus Security Breach

Optus, also referred to as Singtel Optus Pty Limited, is a premier telecommunications company situated in Australia. Optus has a subscriber base of 11 million individuals, representing nearly 40% of Australia's population (Turnbull, 2022). On September 22nd, 2022, the company experienced a security breach, compromising sensitive personal information. 11 million customers were affected by the data breach. There are three key factors that enabled this attack to occur.

1. The data breach occurred through an unprotected and open API. The API used in the attack didn’t require user authentication before establishing a connection, meaning anyone that found the API could connect to and exploit it without submitting a username or password. This security flaw is called broken access control. This factor can be attributed to a misconfiguration (Kost, 2022).

2. The API used to exploit Optus allowed access to backend services that are called on, to get sensitive user account information. The vulnerable API is like the API’s customers use when signing into their account either via through the Optus website or mobile app. This allowed the attacker to access and make requests to the customers database. Below is a list of the data that was compromised (Kost, 2022).

- Driver’s license numbers
- Phone numbers
- Email addresses
- Medicare card
- Passport numbers
- Names
- Dates of birth
- Home addresses

3. The final key factor is how the customers identifies were assigned in the database. Each identifier for the customers was just incremented by one meaning if one customer had an identifier of 25, the next customer would have an identifier of 26. Incrementing identifiers is considered bad programming practice as it enables the attacker to write a script to request the customers information and increment the customer identifier by one which make the data exfiltration process for the attacker easy (Kost, 2022).

In summary, the first security problem Optus had was a misconfiguration of an API that also had broken access control because it didn’t require user authentication to access it. The next security issue was what information the misconfigured API could access. The API could call on backend services that were responsible for retrieving customer information from the customer database. The last security issue Optus had was how their database assigned identifies to customers which was done by incrementing the last customer identifier by one which would become identifier for a new customers. This is bad programming practice because if a database with this setup, is compromised it is easy for an attacker to write a script to take advantage of it.

Optus Breach Severity

Applying the outlined severity criteria, the first factor would score 3 meaning it’s a high risk. This is due to the breach being caused by misconfigurations, broken access control and bad programming practices. The data breach Optus experience could have been easily avoided by proper asset management. Locating old API’s that have access to backend services should always be a security precaution companies follow. Effective access controls should be implemented into the compromised API. A zero-trust model would be a secure method as it assumes that everyone on the company network can’t be trusted and need to prove their identity before being able to access sensitive information. Their database programming practices need to be improved. Random or pseudo random identifiers should be assigned to customers, not an incrementing identifier.

The second factor would focus on what data was exposed in the breach and what are the aftereffects on customers. In the case of the Optus breach Driver’s license numbers, Phone numbers, Email addresses, Medicare card, Passport numbers, Names, Dates of birth, Home addresses were exposed. This type of sensitive information can result in identify theft, phishing attacks and compromised corporate emails which it did. There was a rise in phishing attacks and fraud attempts among the people whose information was exposed. Due to the information that was exposed this factor has a rank of 4, meaning its high risk.

The last factor focuses on how Optus responded to the breach and if they implemented sufficient safeguards to prevent future attacks. Optus reported the breach quickly and held a press conference the day after the breach was reported. They also released a statement informing Optus customers what to do next. They also contacted individuals that had a great risk of fraud or identity theft and informed them how they could protect themselves. For this factor I gave it a score of 1 meaning low risk. They informed the public quickly of the data breach, they also provided statements helping Optus customers to secure their information. This helped with mitigating the aftereffects.

Optus breach severity score: 8/12.

Microsoft Exchange Server Breach

Microsoft exchange server is a mail, calendaring, contact and scheduling platform exclusively used on windows. On January 6, 2021, attacks began on the Microsoft exchange servers and the lasted two months without detection. Multiple groups were involved in the attack and on March 2, Microsoft became aware of the vulnerabilities and provided patches for them. Below is a list of servers that are affected by the vulnerabilities (Pitney, et al., 2022).

- Microsoft Exchange Server 2013
- Microsoft Exchange Server 2016
- Microsoft Exchange Server 2019

There were 60,000 exchange servers comprised, and the type of organisations the servers belonged to range from government, military, manufacturing, and healthcare. The affected exchange servers were in the United States, UK, Germany, Netherlands, and Russia. Many of the compromised servers had ransomware installed onto it and the data extracted from servers were used to blackmail people. Crypto mining botnets were also deployed onto some of servers. Backdoors were also installed in the servers allowing the attackers to gain access to the comprised servers even after the vulnerabilities were patched (Pitney, et al., 2022). The attack was enabled by the attackers using four zero-day vulnerabilities. Below is the list of these vulnerabilities and their Common Vulnerability Scoring System score.

1. CVE-2021-26855
   CVSS: 9.1 (Critical)
   This vulnerability is known as a server-side-request-forgery (SSRF) vulnerability. It allows an attacker to supply a URL which will be read by the server which can result in the server side application to make request to locations it should be able to. This vulnerability was essential in the data breach as it acted as an entry point for the following vulnerabilities to work (NIST, 2021).

2. CVE-2021-26857
   CVSS: 7.8 (High)
   This is a deserialisation vulnerability and when used it will grant the attacker code execution privileges as SYSTEM. The SYSTEM is an account used the by the windows operating system and other services (NIST, 2021).

3. CVE-2021-26858
   CVSS: 7.8 (High)
   This vulnerability allows attackers to deploy web shells which allows backdoors connections to allow remote access to a system. When an attacker has access, they can deploy ransomware attacks or steal user credentials and more (NIST, 2021).

4. CVE-2021-27065
   CVSS: 7.8 (High)
   This vulnerability provides attacks with similar methods of attacks to CVE-2021-27065 (NIST, 2021).

In summary, the Microsoft data breach involved the use of multiple zero-day vulnerabilities and CVE-2021-26855 acted as an entry point for the other vulnerabilities to work. Many organisations were affected globally. When the servers were comprised many different attack methods were utilised ranging from crypto mining botnets, ransomware, and backdoors. This data breach could've been avoided by employing a zero-trust model which treats every user on the network as untrusted until their device is authenticated. This helps prevent lateral movements and internal advancements within systems and grants better access control (Pitney, et al., 2022).

Microsoft Exchange Server Breach Severity

This breach occurred because of four zero-day vulnerabilities being exploited and gave attackers access to the listed exchange servers above. 60,000 servers were affected but this number could be higher. Healthcare, government, military, and finance organisations were attacked and some of the servers had ransomware, crypto mining botnets and backdoors installed on them. The data on the affected servers was also extracted. Because of the extent of the breach the first factor scored 4.

Due to the amount of servers compromised and the privilege levels the vulnerabilities gave the attackers any information on the servers were compromised and extracted. Organization emails accounts were also compromised which may have resulted in sensitive documents being extracted . Due to these reasons this factor scores 3.

A company called DEVCORE told Microsoft about the vulnerabilities on January 5th before the attacks started to happen. On February 8th Microsoft acknowledged that the attacks have escalated and became a serious threat, but a patch wasn't released until March 2nd to address the exploits. Microsoft took one month to fix the exploits used to gain access to 60,000 servers which is a considerable amount of time (Pitney, et al., 2022). When ranking this factor, I am unsure if the above is a normal timeline for companies to release security patches or if Microsoft underestimated the severity of the exploits so for now, I'll rank the third factor with a 3.

Microsoft Exchange Server breach severity score: 10/12.

Bibliography

Kost, E., 2022. *How Did the Optus Data Breach Happen?.* [Online]
Available at: https://www.upguard.com/blog/how-did-the-optus-data-breach-happen#toc-1
[Accessed 11 February 2023].

NIST, 2021. *CVE-2021-26855 Detail.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-26855
[Accessed 9 February 2023].

NIST, 2021. *CVE-2021-26857 Detail.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/cve-2021-26857
[Accessed 9 February 2023].

NIST, 2021. *CVE-2021-26858 Detail.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-26858
[Accessed 9 February 2023].

NIST, 2021. *CVE-2021-27065 Detail.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2021-27065
[Accessed 9 February 2023].

Pitney, A. M., Penrod, S., Foraker, M. & Bhunia, S., 2022. *A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities.* s.l.:IEEE.

Turnbull, T., 2022. *Optus: How a massive data breach has exposed Australia.* [Online]
Available at: https://www.bbc.com/news/world-australia-63056838
[Accessed 15 February 2023].