Anthem Data Breach Analysis

Cybersecurity Management Course

Federica Consoli MAT. 1538420

June 21, 2018

Abstract

The goal of this report is to...

1 How did it happen?

- **Email Security & Protection:** due to the popularity of emails as attack vectos, best practices and special systems are needed to mitigate such a risk.
- **Security Awareness Training:** all employees should be educated on corporate policies, procedures and best practices with regards to information security
- **Privileged Access Management:** administrative privileges on computers, networks and applications should be assigned and managed properly, according to the principle of least privilege.
- **Logging & Auditing:** logging should be enabled on every system and the collected logs should be aggregated and to identify anomalies and abnormal events.
- **Vulnerability Management:** systems should be regurarly scanned in order to identify, classify, remediate and mitigate vulnerabilities.
- **Data Loss Prevention:** data exfiltration is prevented by monitoring data while in-use (endpoint), in-motion (network traffic) and at rest (data storage).

2 Attack Lifecycle

As discussed in the article, the root cause for the data breach that affected Anthem in 2014 is *spear phishing*. According to the reconstruction of the events, the attackers gathered as many information as possible about the tech employees (via Facebook, Linkedin and such) and then used said information to craft a legitimate-looking email with a malicious attachment.
The employees were tricked into opening the attachment, consequentially providing the attackers with remote access to the machine.

Why did this happen? First of all, the users' behaviour shows a lack of *awareness training*. Users are believed to be the weakest link, so companies should have an awareness training program in place to educate them about corporate policies, procedures and best practices with regards to information security.
A thorough awareness training would have provided employees with the ability to recognize a non-legitimate email and report it to the appropriate department, without opening the attachment.

It also appears that Anthem did not have any solutions for *email security* on their network. A Secure Email Gateway, for example, could have provided protection against phishing emails by means of signature-based and sandboxing inspections of the attachment and email authentication methods to detect

spoofing.

The malware contained in the email was probably especially crafted for the attack, so even if the company had an *anti-virus* solution in place it may not have been useful, as the malware's signature would probably not match any entry in the signature database. It is not clear whether *two-factor authentication (2FA)* was enabled or not: a lack of 2FA would definitely make it easier to perform such an attack, but it does not really make much of a difference in the scenario presented, since the attacker infected a machine residing on the corporate network.

After the first initial compromise, the attacker was able to perform privilege escalation. This suggests that the company did not have any form of *privileged access management* in place, that would have prevented applications to run with administrative privileges. Another solution could have been using a *privileged access workstation*, which provides a dedicated and secured operating system to performe sensitive and privileged operations [1].

The attackers were then able to move laterally and compromising more accounts. This was probably made possible by exploting vulnerabilities affecting systems on the network. As some audits [2] showed, Anthem had numerous servers either unpatched or running unsupported operating systems: this shows a lack of a proper vulnerability assessment and mitigation process. Systems and networks should be scanned reguarly in order to verify potentially exploitable vulnerabilities.

1. ~~No email gateway systems~~
2. No system audit / SIEM
3. ~~priviliges management / access control / NEED TO KNOW~~
4. no exfiltration control
5. ~~no routine scanning for vulnerabilities~~
6. no monitor of database activity

References

[1] Microsoft Fundation, ed. *Privileged Access Workstation*. 2016. URL: `https://docs.microsoft.com/en-gb/windows-server/identity/securing-privileged-access/privileged-access-workstations`.

[2] U.S. Office of Personnel Management. *Audit of the Information Systems General and Application Controls at Anthe Blue Cross Blue Shield*. 2016. URL: `https://www.opm.gov/our-inspector-general/reports/2016/audit-of-the-information-systems-general-and-application-controls-at-anthem-blue-cross-blue-shield.pdf`.