Anthem Data Breach Analysis

Cybersecurity Management Course

Federica Consoli
Matricola 1538420

June 25, 2018

Contents

1 Introduction

The goal of this report is to discuss the data breach that affected Anthem (the second largest health insurer in the United States) in 2014. In the first section, I will offer an insight on which security controls were either missing or implemented inadequately.
Then, in the second section, I will reconstruct the attack lifecycle and discuss, at each stage, what allowed it to happen and how the aforementioned security controls could have prevented it.

2 Security Controls

Upon reading Steve Ragan's article [1] describing the nature of the breach that affected Anthem, it appears that the company's security measures were both insufficient and inadequate. This means that it was not only a matter of *which* controls were missing: the ones that were actually in place may have not been configured or even used properly.

From what I gathered, the following security measures were either missing or not properly implemented at the time of the attack.

2.1 Email Security

The article states that the attack was initiated using a phishing email with a malicious attachment. Due to the popularity of emails as attack vectors, company should take appropriate measures to mitigate such risks, by means of specialized systems as Secure Email Gateway, sophisticated spam filters and so on.

2.2 Security Awareness Training

It is unclear whether Anthem had a Security Awareness program in place for their employees. However, even if there was, it was clearly inadequate. All employees, especially those with access to critical systems, should be educated on corporate policies, procedures and best practices with regards to information security.

2.3 Privileged Access Management

Administrative privileges on computers, networks and applications should be assigned and managed properly, according to the principle of least privilege. Moreover, the company should have full visibility and control over all privileged accounts across their assets. This serves two purposes, mitigating the risks posed by insider threats and preventing data breaches.

2.4 Logging & Auditing

Logging should be enabled on every system for security purposes. Logs should be collected, aggregated and analyzed in order to identify anomalies and abnormal events.

2.5 Vulnerability Management

Companies should have a thorough vulnerability assessment/management progeam in place. Systems should be scanned regurarly in order to identify, classify and mitigate vulnerabilities.

2.6 Data Loss Prevention

In order to prevent exfiltration, data should be monitored at all stages: in-use, in-motion and at rest. DLP solutions are focused on preventing unauthorized access, abnormal use and unauthorized copies/leakage.

3 Ethical Implications

The evolution of computer and technology surely made life easier under several aspects both for individuals and businesses, but it does not come without a price. This is why a new branch of applied ethics was created, called *computer ethics*: the term was conied by Walter Maner in the mid-70s, and it refers to the study of all those ethical problems "aggravated, transformed or created by computer technology"[2].

Companies that try to enforce some of the security controls mentioned in the previous section cannot do so without taking into consideration the ethical issues that come with them, which are illustrated in the following sections.

3.1 Email Security

First and foremost, certain controls might affect the *privacy* of the employees. As discussed before, it might be important to monitor the exchange of emails in order to identify potentially malicious messages. There are several considerations to be made:

- Is it ethical for a company to access employees email, even if it is to avoid loss/theft of sensitive corporate data?
- Should the company be able to read the content of the email? Or should they have access only to headers and attachments?
- Should employees be allowed to access their personal email account while at work? If so, should the company monitor both personal and professional emails?
- Should this policy be disclosed to employees?

- privacy & monitoring
- whistle-blower policy?

Discuss which information security ethical principles would apply to the control weaknesses identified in the previous step 2 [GUIDANCE: Please reference the set of slides N.3 on "Ethics"]; the purpose of question in point 3 is for you to analyze and comment on the ethical implications of the controls

recommended by the relevant information security standards and frameworks studied during our classes (and/or any other relevant source of best practices that you may want to reference). For example, the activities of staff when using the ICT assets of an organization may be monitored. What are the ethical considerations (and/or mitigating measures) of such an approach?

On a more general level, ethics must also be considered when utilizing security solutions that have administrative access to employees' personal devices when they're being used in conjunction with a bring-your-own-device policy, such as mobile device management and network access control systems. Those hoping to join the cybersecurity profession will need to comprehend all aspects of ethics' relationship with IT and make these practices a natural part of their working behavior.

4 The Attack

As discussed in the article, the root cause for the data breach is *spear phishing*. According to the reconstruction of the events, the attackers gathered as many information as possible about a couple of 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*. As mentioned before, 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[3].

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[4] showed, Anthem had numerous servers either unpatched or running unsupported operating systems: this shows a lack of a proper *vulnerability assessment/mitigation process*. Systems should be scanned reguarly and kept up-to-date with security patches; moreover, end-of-life hardware and software should be replaced.

It is also interesting to point out that the intrusion was only detected because an employee noticed a query on the database they did not initiate. This shows a lack of several security controls. First of all, the company probably did not collect logs to be used in a *Security Information and Event Management (SIEM)*. SIEMs provide visibility on the whole company by storing, analyzing and correlating different types of security events (authentication events, anti-virus events, intrusion events...). Moreover, SIEMs can be tuned by specifying rules and "normal" behaviour. Any suspicious activity would be promptly picked up, generating an alert requiring immediate action.

User Behaviour Analytics (UBA) software focuses on a range of specific user activities [5] in order to identify abnormal user behaviour that may indicate that the account was compromised. UBA software usually compares current user activity to their historic activity and the activity of other users in similar roles; moreover, it might check things like the location of the session and the time of the day, even if the credential was authenticated through valid (phished) credentials. This kind of software helps mitigate the risks of both insider and ousider threats.

After successfully accessing the database, the attackers reportedly were able to expose over 80 million customer records, completely unnoticed. The attackers were able to do so because Anthem was lacking *Data Loss Prevention (DLP)* controls. This includes traffic monitoring and analysis at egress point near the perementer, to detect sensitive or confidential data that is being sent in violation of security policies.

5 Standards

Referencing the ISO27001/2 standard or any other information security standard/best practices/frameworks of your choice (i.e., TOP 20 Critical Controls; NIST Series 800; etc.), describe at least five (5) controls that would have mitigated the weaknesses identified, how and why

6 Conclusions

Conclude your analysis with summary observations about any potential limitations presented by the referenced information security standard/best practices/frameworks

7 References

[1] Steve Ragan. "Anthem: How does a breach like this happen?" In: (2015). Ed. by CSO Online. URL: https://www.csoonline.com/article/2881532/business-continuity/anthem-how-does-a-breach-like-this-happen.html.

[2] Herman T. Tavani Richard A. Spinello. *Readings in CyberEthics*. Ed. by Jones and Bartlett Publisher. 2nd ed. 2004, p. 18.

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

[4] 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.

[5] Cindy Ng. *The Difference Between SIEM and UBA*. URL: https://blog.varonis.com/the-difference-between-siem-and-uba/.