Anthem Data Breach Analysis

Cybersecurity Management Course

Federica Consoli
Matricola 1538420

June 30, 2018

Contents

1 Introduction

The goal of this assignment is to discuss the data breach that affected Anthem, the second largest health insurer in the United States, in 2014. The report will focus on how the attack was carried out, what weaknesses were exploited and what should have been done to prevent and mitigate it.

The documents is structured as follows:

- The *second* paragraph contains an analysis on the control weaknesses that exposed the organization to the attack, as described in the article "Anthem: How does a breach like this happen?"[1]. For each of the identified controls, there is a short description and an explanation of why they should have been implemented.

- The *third* paragraph focuses on the topic of computer ethics. Ethical issues will be presented with reference to the control weaknesses identified in the previous section, explaining how and why they might affect the company.

- The *fourth* paragraph offers a reconstruction of the life cycle of the attack, starting from the initial compromise all the way through the exfiltration of stolen data. This will be done by referencing the weaknesses discussed in section two, explaining how the attackers exploited them and what the consequences were.

- The *fifth* paragraph is be centered around how (and why) following information security standars/best practices would have mitigated the vulnerabilities that caused the company to be attacked. The document I chose for this purpose was the "Top 20 Critical Controls" by the Center for Internet Security (CIS): starting from this standard, I chose six different controls and discussed their relationship to the weaknesses that affected Anthem.

- The *sixth* paragraph is dedicated to a conclusive analysis of the potential limitations of the CIS controls that were illustrated in the previous section of the document, explaining why they are not enough to ensure security.

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 company was affected by the following weaknesses:

2.1 Email and Web Security

Due to the popularity of emails as attack vectors, companies should take appropriate measures to mitigate such risks, by using specialized systems as Secure Email Gateway, sophisticated spam filters and so on. This would have provided protection against phishing emails by means of signature-based and sandboxing inspections of the attachment and email authentication methods to detect spoofing.

In addition to that, it is crucial to monitor user activity on the Internet (for example through the use of a web proxy), in order to prevent employees from accessing malicious websites that could compromise their machines.

2.2 Endpoint Security

Endpoint Protection solutions allow enterprises to secure user workstations and prevent even the more sophisticated attacks. This kind of solution may involve monitoring user activities to define a pattern of “normal” user behaviour, which would be later used as a comparison to detect anomalies.

Other solutions may include Host Intrusion Detection and Prevention Systems (HIPS/HIDS) and next-generation antiviruses: the goal of such solutions is to detect malicious files and applications and promptly block their execution.

2.3 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 regurarly educated on corporate policies, procedures and best practices with regards to information security.

2.4 Management of Administrative Privileges

Administrative privileges on computers, networks and applications should be assigned and managed properly, according to the principle of least privilege (meaning that employees should be given access to the minimum set of information needed to perform their job). Moreover, the company should have full visibility and control over all privileged accounts across their assets, which serves two purposes: mitigating the risks posed by insider threats and preventing data breaches.

2.5 Logs Review

Logging should be enabled on every system for security purposes, especially on critical assets containing sensitive business data. Logs should be collected, aggregated and analyzed in order to identify anomalies and abnormal events. Review of logs could allow security professional to detect intrusions and unauthorized access and provide complete visibility over what is happening in the corporate network.

2.6 Vulnerability Management Process

Companies should have a thorough vulnerability assessment/management program in place. Systems should be scanned regurarly in order to identify, classify and mitigate vulnerabilities. Moreover, operating systems and applications should be kept up-to-date with security patches and updates.

2.7 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: these solutions may include next-generation firewalls, e-mail gateways, web proxies and so on.

3 Ethical Implications

The evolution of computer and technology certainly made life easier 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 and Web 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 their employees' emails, 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?

Similar issues affect the monitoring of web activity through the use, for example, of web proxies. Although the ultimate goal is to ensure the security of corporate data, the following questions arise:

- Is it ethical for companies to access the web history of their employees?
- Should such data be logged? If so, who should be able to access it?
- If something problematic were to be found, should management be involved? Even if it means to jeopardize the employee's reputation?

3.2 Endpoint Security

Employees may also be affected by the adoption of endpoint security solutions. As mentioned before, certain systems may incorporate analysis of user behaviour: this is done by using a type of software that monitors the user's activity under normal system conditions and keeps track of other information such as date, time and location of login events. This data is then used to generate a profile of what is considered to be a regular set of activities inside the system, and every behaviour that deviates from this will trigger an alert.

There are several ethical cosiderations to be made about this approach:

- Should companies use such solutions, even if they might affect the overall performance of the system, causing disturbance or disruption of staff activities?
- Is it ethical for companies to use software that performs keystroke analysis to better determine the profile of a user, since this actually means having a keylogger installed on the employee's machine?
- Should companies be able to collect data about user's location and date/time of login events? Or is it a violation of privacy?

3.3 Security Awareness

The goal of Security Awareness is educate employees on what information security is and why it should be considered an integrant part of the business, providing knowledge about corporate policies and regulations at the same time. It should be clear for employees what their jobs and duties are, and most importantly who to contact if they notice something suspicious or potentially malicious.

This includes what are commonly called *whistleblowing policies*. The term "whistleblower" is used to indicate an employee that reports misconduct to people or entities that could take corrective action. Whistleblower policies are needed to make sure that employees have an anonymous way to report illegal practices or violations of corporate policies, without fearing any form of retaliation or discrimination.

The topic of whistleblowers is a delicate one, since there is a clear ethical conflict: on one hand, there is loyalty to the employer, while on the other there is loyalty to one's moral principles.

4 The Attack

After discussing what weaknesses were affecting Anthem, this section offers an insight on how the attack was carried out and how the aforementioned weaknesses were exploited by the attackers.

4.1 Initial Compromise

As discussed in the article, the root cause for the data breach was *spear phishing*. According to the recollection of the events, the attackers gathered as many information as possible about a couple of employees in technical roles (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 their machine.

This was possible for two reasons: first of all, employees did not receive a thorough *security awareness training* that would have provided them with the ability to recognize non-legitimate emails and to report them. Secondly, Anthem did not deploy any solution for *email security* on their network, which could have analyzed and detected the malicious attachment before it could reach the user's mailbox.

4.2 Privilege Escalation & Lateral Movement

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 from running with administrative privileges.

The attackers were then able to move laterally and compromise even more accounts. This was probably made possible by exploting vulnerabilities affecting systems on the network. As some audits [3] showed, Anthem had numerous servers either unpatched or running unsupported operating systems version: this shows a lack of a proper *vulnerability assessment/mitigation process.*

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 that prevented Anthem from having complete *visibility* over what was happening on their systems.

First of all, even if the company probably did collect logs from several systems on the network, the review process of said logs was not appropriate: logs should be reviewed on a daily basis, either manually or by deploying a Security Information and Event Management (SIEM), in order to identify unusual activities that might mean that the system was compromised.

Moreover, the company probably did not deploy any kind of *User Behaviour Analytics* system: this type of software could have picked up abnormal user behaviour (e.g. unusual login time and/or location, unusual activity - compared to what the employee usually does) and trigger an alert.

4.3 Data Exfiltration

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 monitoring and analyzing the network traffick at egress point near the perementer, in order to detect sensitive or confidential data that is being transferred in violation of security policies.

5 Standards

The Center for Internet Security (CIS) provides a set of twenty security controls and best practices aimed at mitigating the most common attacks against systems and networks, helping companies to improve their overall security state [4].

Following are six controls that Anthem should have implemented: for each of them, there is a short explanation of what they are and how they would have helped to prevent the breach.

5.1 CSC 3: Continuous Vulnerability Assessment

"Continuously acquire, assess and take action on new information in order to identify vulnerabilities and to remediate and minimize the window of opportunity for attackers."

By using automated vulnerability scanning tools (controls 3.1 and 3.2), Anthem could have promptly discovered misconfigurations and/or vulnerabilities and addressed them in a proactive manner, drastically reducing the attack surface.

Moreover, the deployment of an automated software update solution (controls 3.4 and 3.5) would have kept operating systems and applications up-to-date with security patches, making it difficult for the attackers to move laterally in the organization by exploiting vulnerable systems.

5.2 CSC 4: Controlled Use of Administrative Privileges

"Track, control, prevent and correct the use, assignment and configuration of administrative privileges on computers, networks and applications."

This control could have helped Anthem to prevent attackers from performing privilege escalation. For example, controls 4.3 and 4.6 suggest using a dedicated account and/or workstation: these would be used only to perform administrative tasks, with no Internet access and no possibility of using emails, web browsers and so on.

5.3 CSC 6: Maintenance, Monitoring and Analysis of Audit Logs

"Collect, manage and analyze audit logs of events that could help detect, understand or recover from an attack."

The absence of clear and detailed logs allows attackers to hide their presence and activity on the victim's systems: in Anthem's case, the breach was only discovered "by accident" because an employee noticed a suspicious query on the database.

Control 6.6 suggests the deployment of a SIEM to allow log correlation and analysis, while control 6.8 says that the SIEM should be tuned regurarly to allow better identification of events and decrease unnecessary noise. Moreover, control 6.7 states that logs should be reviewed regurarly to identify anomalies and/or abnormal events in the system: Anthem failed to do this, and it is the reason why the company was not able to detect the compromise rightaway.

5.4 CSC 7: Email and Web Browser Protections

"Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and e-mail systems."

Web browser and email clients are very common points of attack, since they represent the main means of interaction between users and untrusted environments. With reference to Anthem's case, controls 7.9 and 7.10 definitely could have helped to mitigate the risk of spear phishing emails. The former suggests blocking all email attachments reaching the corporate's gateway if the file type is not necessary for the business, while the latter advocates for the use of sandbox analysis of inbound emails to identify and block attachments which appears to be malicious.

Moreover, control 7.8 suggests enabling receiver-side verification and spam-filtering tools to improve security against spoofed and phishing emails: as an example, this can be done by implementing Domain-based Message Authentication, Reporting and Conformance (DMARC) and Sender Policy Framework (SPF).

The implementation of said controls would have helped the company to prevent the attackers from launching the attack, since the malicious attachment would have never reached the employee's mailbox in the first place.

5.5 CSC 13: Data Protection

"Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information."

The main goal of this control is the creation of an inventory containing all sensitive data/assets (control 13.1), in order to separate them from less sensitive information. Moreover, it is suggested to segment the network so that systems of the same sensitivity level are on the same segment but also separated from systems with a different level.

This allows fine-grained access control on a need-to-know basis, meaning that employees are allowed to access only the information they need to perform their jobs. Such approach could have helped in Anthem case, because it would have prevented a single employee from having access to an entire database containing customer records.

Moreover, control 13.3 states the importance of monitoring and blocking unauthorized network traffic by deploying automated tools on the company perimeters: this would have allowed Anthem to detect the unauthorized transfer of their sensitive records and to promptly block the exfiltration of data.

5.6 CSC 17: Security Awareness and Training Program

"Identify the specific knowledge, skills and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training and awareness programs for all functional roles in the organization."

This control aims at providing all functional roles within an organization with "good cyber defense habits" that could increase readiness and responsiveness to attacks. As stated in the CIS document, companies should take a holistic approach that does not only consider policy and technology, but also focuses on training employees. Even in Anthem's case, the training should have been tailored to each employee's role and responsibility, and it should have been repeated and updated regularly, as stated in controls 17.3 and 17.4.

Control 17.6 focuses on the need to train the employees on how to identify social engineering attacks, such as phishing and impersonation calls: this control would have clearly helped Anthem to prevent the attack, since the compromise was made possible by exploiting the human factor and tricking employees into opening a phishing email. Finally, control 17.9 states the importance of training employees on how to identify the most common indicators of an incident in order to report it: this could have helped employees in technical roles to discover the breach earlier and to minimize its impact.

6 Conclusions

To conclude this analysis, it is worth explaining why the CIS Critical Security Controls alone are not enough to keep an organization safe. First of all, the document only presents a summary of what controls should be implemented, with little to no details on how it should be done. Moreover, security controls are described in a "one size fits all" manner, even if the reality strays far from that: each organization is different, depending on the business area they operate in and the type of information they deal with.

This means that a certain level of security expertise is needed to tailor the controls to the organization's needs before implementing them: this should involve a risk assessment process, where security professionals review and prioritize their critical assets and data and decides which security controls are the most relevant to their case.

Finally, it is also important to stress that implementing the controls suggested by CIS or any other information security framework does not automatically means that the organization is secure, it just indicates compliance with said standards. Controls (together with staff!) should be constantly reviewed, updated and tuned in order to keep up with the ever-evolving scenario of threats and cyber attacks.

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] 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.

[4] Center for Internet Security. *CIS Controls Version 7*. URL: https://learn.cisecurity.org/20-controls-download.