

Anthem Data Breach Analysis
Cybersecurity Management Course

Federica Consoli MAT. 1538420

June 19, 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 vectors, 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
- **Privilege Control:** 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 regularly 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

2.1 Initial compromise

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 much 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.

2.2 Privilege escalation and lateral movement

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* 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 compro

2.3 Data Exfiltration

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