BANK INFO SECURITY®

https://www.bankinfosecurity.com/

Anti-Phishing, DMARC , Fraud Management & Cybercrime , Governance & Risk Management

A New In-Depth Analysis of Anthem Breach

Insurance Commissioners Conclude Nation-State Involved, Reach Settlement with Insurer

Marianne Kolbasuk McGee (HealthInfoSec) • January 10, 2017

Seven state insurance commissioners, in a new report on their investigation into the massive cyberattack against health insurer Anthem Inc. in February 2015, offer a detailed account of what happened in the incident, which began with a phishing campaign. They conclude, as had already been widely speculated, that a nation-state was behind the attack, which affected 78.8 million individuals. But they stop short of naming the nation involved.

See Also: Fireside Chat | The Evolution of Threat Hunting and Why it's More Important Now Than Ever

The commissioners also announced they reached a regulatory settlement agreement with the insurer that did not impose any fines but called on the company to make significant investments in security enhancements. Anthem is spending more than $260 million on those security-related measures, the report notes.

"Our examination team concluded with a significant degree of confidence that the cyberattacker was acting on behalf of a foreign government," California Insurance Commissioner Dave Jones says in a statement.

"Insurers and regulators alone cannot stop foreign government assisted cyberattacks," he says. "The United States government needs to take steps to prevent and hold foreign governments and other foreign actors accountable for cyberattacks on insurers, much as the president did in response to Russian government sponsored cyber hacking in our recent presidential election." (See *Russian Election Related Hacking Details Declassified*).

The California Department of Insurance took the lead in releasing on Jan. 6 a report outlining the investigation's findings, plus a regulatory settlement agreement.

The settlement document notes that Anthem "has already incurred significant costs related to the data breach." That includes $2.5 million to engage expert consultants; $115 million for the implementation of security improvements; $31 million to provide initial notification to the public and affected individuals; and $112 million to provide credit protection to breach-impacted consumers. "The company and the lead states have also agreed upon additional security enhancements and further efforts to assist breach-affected individuals," the document notes.

Breach Investigation Findings

The insurance commissioners employed an examination team that included the cybersecurity firm CrowdStrike and Alvarez & Marsal Insurance and Risk Advisory Services. The team focused its investigation on Anthem's pre-breach response preparedness, the company's response adequacy at the time of the breach and its post-breach response and corrective actions, the California Department of Insurance statement notes.

The investigation by the insurance commissioners' examination team - and a separate internal investigation by security firm Mandiant, which Anthem hired - determined the data breach began on Feb. 18, 2014, when a user within one of Anthem's subsidiaries opened a phishing email containing malicious content.

Opening the email launched the download of malicious files to the user's computer and allowed hackers to gain remote access to that computer and dozens of other systems within the Anthem enterprise, including Anthem's data warehouse, the commissioners' investigation report says.

Starting with the initial remote access, the attacker was able to move laterally across Anthem systems and escalate privileges, gaining increasingly greater ability to access information and make changes in Anthem's environment, the investigative report says.

"The attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the company's enterprise data warehouse - a system that stores a large amount of consumer personally identifiable

information," the report notes. "Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 million unique user records."

The investigation team found that Anthem had taken reasonable measures before the data breach to protect its data and employed a remediation plan resulting in a rapid and effective response to the breach once it was discovered. The team worked with Anthem to develop a plan to address its security vulnerabilities and conducted a penetration test exercise to validate the strength of Anthem's corrective measures. As a result, the team found Anthem's improvements to its cybersecurity protocols and planned improvements were reasonable, the report notes.

Nation-State Attacker

"The team determined with a high degree of confidence the identity of the attacker and concluded with a medium degree of confidence that the attacker was acting on behalf of a foreign government," the report states. "Notably, the exam team also advised that previous attacks associated with this foreign government have not resulted in personal information being transferred to non-state actors."

The report does not identify the nation-state suspected in the attack.

Herb Lin, senior research scholar for cyber policy and security at the Center for International Security and Cooperation, a think tank at Stanford University, notes, however, that China had been suspected as being involved in the attack when it was revealed in 2015. "It could have been China, it could have been Russia or another country. But China has a vibrant biotechnology [industry] where healthcare information could be competitively relevant to them," he notes.

Privacy attorney Adam Greene of the law firm Davis Wright Tremaine notes: "It's interesting that the California Department of Insurance chose not to identify China in light of earlier press reports suggesting their involvement."

Critiquing the Report

Dan Berger, CEO of security consulting firm Redspin, says he's confident in the findings of the investigation. "I have the same degree of confidence as the investigators that this attack was orchestrated by a nation-state," he says. "The sophistication of the attack evident not

from the phishing email but from the ability of the malware to move laterally throughout the IT infrastructure, access critical databases, and exfiltrate date - all without detection."

As for the settlement between Anthem and the insurance commissioners, "I see this settlement as good news for Anthem," Greene says. "The states found that administrative fines or penalties were not warranted, and that Anthem's money is better spent on cybersecurity than on 'punitive or exemplary fines.' Anthem may try to use this as evidence in [ongoing class action] litigation that they acted responsibly and that punitive damages are not appropriate," he notes (see *Those Suing Anthem Seek Security Audit Documents*).

Lessons Learned

Other healthcare sector organizations also can learn from the Anthem investigation report, security experts note.

"The fact that the investigation revealed that a breach of this magnitude began with a phishing email underscores the importance of comprehensive and frequent security awareness training for all employees of healthcare organizations," Berger says.

"The human 'perimeter' again and again appears to be the weakest link. This isn't easy - the attackers can send hundreds if not thousands of emails over time and it only takes one to get through."

Keith Fricke, principal consultant at tw-Security, adds: "There are no guarantees that social engineering awareness training will 100 percent prevent successful social engineering attacks, but it will help reduce the risk. Using and maintaining advanced malware protection and patching security vulnerabilities remain important as risk management measures."

Bolstering Security

In terms of the money Anthem has been spending in bolstering security in the wake of the breach, "Anthem is making a large but proportionate investment," Berger says. "I expect other healthcare organizations to take note and hopefully that will translate into increased IT security budgets sooner rather than later."

The insurance commissioner's report notes that Anthem has implemented two-factor authentication on all remote access tools, deployed a privileged account management solution and added enhanced logging resources to its security event and incident management solutions.

"Further, the company conducted a complete reset of passwords for all privileged users, suspended all remote access pending implementation of two-factor authentication and created new Network Admin IDs to replace existing IDs," the report notes. "Anthem acquired additional technology to improve its monitoring capabilities in critical databases."

The report also points out that the examination team noted "exploitable vulnerabilities in the immediate aftermath of the data breach, and that Anthem had developed a remediation plan to address those issues. It is the examination team's view that Anthem's improvements to its cybersecurity protocols and schedule of planned future improvements appeared to be reasonable efforts to secure the environment beyond the initial data breach remediation tasks."

Mac McMillan, CEO of security consulting firm CynergisTek, says Anthem appears to be taking the right critical steps to bolster its security. "The Anthem breach and investigation afterward demonstrate how important it is for organizations to clean up and tighten the access control measures and the value of two factor authentication," he notes.

About the Author

Marianne Kolbasuk McGee

Executive Editor, HealthcareInfoSecurity, ISMG

McGee is executive editor of Information Security Media Group's HealthcareInfoSecurity.com media site. She has about 30 years of IT journalism experience, with a focus on healthcare information technology issues for more than 15 years. Before joining ISMG in 2012, she was a reporter at InformationWeek magazine and news site and played a lead role in the launch of InformationWeek's healthcare IT media site.