Alaska Dept Health Case Study

Alaska Department of Health

Passive malware attack

In 18th of May 2021, the Alaska's Department of Health and Social Services (DHSS) reported a security breach with an assumption that it was performed by a sophisticated nation state-level attacker.
The attacker successfully carried out a passive malware attack, (a program that exfiltrate data) with elevated privileges and is speculated to be initiated by phishing emails. Unfortunately, this is not the first attack seen by the DHSS with incidents in 2012, 2017 and 2018.
Beyond surveillance, the attack end objective is unknown, however they had access to all Personally Identifiable Information of all customer profiles (estimate of more than 100000 households), from Social security number to health/financial information (HIPAA).
The department hired Mandiant/FireEye to carry out the independent report. The breach was detected by Alaska's Office of IT on 2nd of May, but only reported to the department on 5th of May. The department decided to shut down all services to deny the attackers any access.

References:
https://dhss.alaska.gov/news/
https://www.govinfosecurity.com/alaska-health-department-servic

The Alaskan DHSS notified the public in general on the 16th of September 2021 on the HIPPA/Alaska Personal Information Protection Act(APIPA) breach.
This is four months since the event.
Alaska’s DHSS key role is to manage healthcare services to the Alaskan public.
Before 2017, the Alaska’s DHSS did not have a Risk Management policy. Since then, the department has hired private firms (Mandiant).
Unfortunately some of the details such as identity of the attackers, method and time are not shared with the public at the moment.
Previous attacks in 2017 and 2018 were carried out using botnets installed after employees were targeted using phising methods.
This incident may be similar, however it is not acknowledged or denied by the government.

Timeline

Alaska DHSS Attack in 2021

1. 2nd May 2021 - Event of Breach detected by security monitoring contractors
2. 5th May 2021 - Event of Breach reported to Alaska's DHSS, iving a 3 day advantage to the attackers to exfiltrate data and full access to the servers
3. 17th May 2021 - Alaska's DHSS shuts down all services that is compromised
4. 18th May 2021 - Alaska's DHSS reports to the public of the incident
5. 7th June 2021 - Alaska's DHSS informs that an root cause analysis would be carried out to investigate the attack
6. 26th July 2021 - Alaska's DHSS restores access to services

Vulnerabilities

A data breach of personal identifiable information (100k Alaskan households) including health records and social security was found on the 2nd of May 2021. The attacker successfully carried out a passive malware attack, (a program that ex-filtrate data)and was speculated to be initiated by phishing emails.

Vulnerability #1

Phishing email events has occurred in the past.

Vulnerability #2

Insufficient Risk Management/Crisis Management capacity within the Alaskan department. All incident reporting is outsourced to private companies

Vulnerability #3

Delay in communication increases the risk that the vulnerability had been exploited

Vulnerability #4

Critical citizen data was not stored securely or guarded once a server and its network has been compromised

Costs

- Possible data from more than 100k households in Alaska has been compromised
- User member login information, medical records, social security, financial and contact info had been compromised
- Monitoring performed by 3rd party service provider with limited budget, influenced by spending politics
- Due to budget cuts, low priority given to local DHSS
- Poor communication between the public and local government

Prevention

- The state has now been liable to a lawsuit of millions and has offered free credit monitoring for suspicious activities. Risk Mgmt and Information Office more focused on security.
- Multi factor authentication has then been in consideration. Isolation of data/resource (limited data access) based on roles.
- Increase in security minded staff needed. More serious approach to risk management
- More investment in competency
- Toll free hot line centers and monitoring services provided