Victoria Kizzee

ITCS 4315

Incident Report: Change Healthcare Ransomware Attack

Contact Information:

Name: Victoria Kizzee

Address: 5000 Research Forest Drive

The Woodlands, Texas 77381

Job Title: Student

Phone: 832.813.6500

Email: VIKIZZE@MY.LONESTAR.EDU

Executive Summary

The ransomware attack on Change Healthcare, a prominent health care payment processor, stands as one of the most serious incidents targeting a U.S. health care organization. The attack disrupted critical services, affecting health care providers, patients, and insurance reimbursement processes. This report outlines the incident, its impact, and recommendations for mitigating future risks.

Background

Change Healthcare is responsible for the flow of payments between payers, providers, and patients in the U.S. healthcare system. It processes billions of transactions annually, making it a critical infrastructure for healthcare operations.

Incident Details

- Date: February 21, 2024
- Target: Change Healthcare (part of Optum and owned by UnitedHealth Group)
- Attack Vector: Ransomware (specifically, Alphy)
- Impact:
    - Most of Change Healthcare's systems were taken offline to prevent further spread.
    - Small and midsize health care providers faced disruptions in electronic prescription filling and insurance reimbursement.
    - Over 70,000 U.S. pharmacies using Change Healthcare's payment processor were affected.
    - Alphy ransomware encrypted critical data, demanding payment for decryption keys.

Timeline

- February 21, 2024: Initial breach detected.
- February 22-28, 2024: Disruption in healthcare payment processing observed.
- March 2024: UnitedHealth, the parent company, begins assessing the damage and costs associated with the attack.

Forensic Analysis

Forensic analysis revealed that the ALPHV group exploited vulnerabilities in Change Healthcare's network to deploy ransomware. Over six terabytes of data were allegedly stolen, including sensitive medical records.

Threat Intelligence

- Alphy Ransomware:
    - Created by Russian-speaking cybercriminals.
    - Previously used in the devastating attack on MGM Resorts in Las Vegas.
    - Mode of installation remains unclear (by a small group of young, English-speaking hackers).
    - Thousands of pharmacies resorted to “offline processing workarounds.”

Incident Response

- Immediate Actions:
    - Change Healthcare isolated affected systems.
    - Developed a new workaround for electronic prescription services.
    - Communicated with affected health care providers and pharmacies.
- Long-Term Measures:
    - Strengthen endpoint security to prevent future ransomware attacks.
    - Regularly update and patch software.
    - Enhance employee training in phishing awareness.
    - Establish robust incident response procedures.

Recommendations

1. Risk Assessment:
    - Conduct a thorough risk assessment to identify vulnerabilities in critical systems.
    - Prioritize protection of patient data, financial transactions, and essential services.

2. Security Controls:
    - Implement role-based access controls to limit system exposure.
    - Deploy end-to-end encryption for sensitive data.
    - Regularly audit and assess security posture.
3. Incident Communication:
    - Establish clear communication channels during incidents.
    - Notify affected parties promptly and transparently.
4. Collaboration:
    - Collaborate with law enforcement agencies and cybersecurity experts.
    - Share threat intelligence to prevent similar attacks.

Containment Actions

UnitedHealth took immediate action to contain the breach, including paying a ransom to prevent data disclosure and implementing measures to restore operations.

Root Cause Analysis

The root cause of the attack was identified as a combination of sophisticated phishing techniques and unpatched security vulnerabilities within Change Healthcare’s network.

Conclusion

The Change Healthcare ransomware attack underscores the critical need for robust cybersecurity measures in the health care sector. By learning from this incident, organizations can better protect patient data, maintain essential services, and respond effectively to future threats.

Cite:

"Ransomware Attack on U.S. Health Care Payment Processor 'Most Serious Incident of Its Kind.'" *NBC News*, 1 Mar. 2024, www.nbcnews.com/tech/security/ransomware-attack-us-health-care-payment-processor-serious-incident-ki-rcna141322.

Storchak, Yana. "Top 10 Best-Known Cybersecurity Incidents | Ekran System." *Ekran System*, 20 Feb. 2024, www.ekransystem.com/en/blog/top-10-cyber-security-breaches.

Jennings, Mike. "Top Data Breaches and Cyber Attacks of 2022." *TechRadar*, 4 May 2022, www.techradar.com/features/top-data-breaches-and-cyber-attacks-of-2022.

Drapkin, Aaron, and Aaron Drapkin. "Data Breaches That Have Happened in 2022, 2023 and 2024 so Far." *Tech.co*, 18 Apr. 2024, tech.co/news/data-breaches-updated-list.