Module 5: Incident Response Management Report

Kyler Kent

School of Continuing Studies, Georgetown University

MPCR-7990-101: Capstone

Dr. Rosemarie Pelletier

October 1, 2023

Module 5: Incident Response Management Report

I will start with the NIST CSF (Cybersecurity Framework) in order to best characterize the Ackme incident (NIST, 2023). The NIST CSF is broken down into the following phases: identify, protect, detect, deter, respond, and recover.

Identify

Ackme appears to have a poor understanding of cybersecurity risk management, as judged by its lack of controls, detection capabilities, and incident response. Ackme appears to be a reactive organization instead of a proactive one. An exception to this could be the fact that Ackme may have prepared to protect its most important resources (i.e., crown jewels) via backups that are allegedly available for restoration (Georgetown University, n.d.-b, para. 2). Using maturity tools like the CMMI (Capability Maturity Model Integration) to assess Ackme's maturity, it is apparent that Ackme is at a stage of infancy, lacking both in maturity and capability (ISACA, n.d.).

Protect

As previously stated, Ackme does not appear to have any formal list of security controls or tools in place to protect or guard its infrastructure from cyber threats. This finding emphasizes the reactive nature of Ackme towards cybersecurity risk management and the broader threat landscape. The FBI appears to be commandeering Ackme's investigation and forcing it to only monitor the attacker's presence without interruption (Georgetown University, n.d.-c, para. 3). Ackme appears to be, in terms of cybersecurity, a weak and vulnerable organization with negotiation capabilities with governmental and regulatory agencies.

Detect

Ackme appears to have poor detection methods in place. Ackme appears to have only learned of the cyber incident via the ransom demand on infected hosts (Georgetown University, n.d.-a, para. 1). Additionally, The FBI was also seen having to provide a comprehensive list of IOCs for Ackme for proper detection of their adversary (Georgetown University, n.d.-c, para. 3). Furthermore, it was also alerted to compromise of it supplier by the supplier itself instead of through its own detection or internal intelligence sources (Georgetown University, n.d.-d). Next, Ackme was supplied with specific IOCs for that incident, such as "split HTTP post requests" (Thexpert, 2019, 02:30-02:32). Ackme does not appear to have mature or established detection methods in place or even the capability to detect and construct IOCs. To improve Ackme's incident response, practices such as threat hunting could allow Ackme to potentially identify and develop the IOCs prior to being notified by third parties (Taschler, 2023).

Respond

The most common motif in Ackme's incident response is reactiveness rather than proactiveness. Since now we have direct information that Ackme has suffered a data breach with sensitive information on individuals, Ackme must perform breach victim notification according to state laws in each of the victim's states (Georgetown University, n.d.-c, para. 1; IT Governance USA, n.d.). Additional notification requirements include notifying the SEC (U.S. Securities and Exchange Commission) as well as public shareholders of the breach via Form 8-K (SEC, 2023). Ackme's business leader's transparency failures have only added insult to injury and will hamper Ackme's public relations during its incident response (Georgetown University, n.d.-c, para. 1).

Recover

Ackme cannot proceed to this phase given the FBI's current instructions (Georgetown University, n.d.-c, para. 3). While Ackme appeared to have plans to restore from backups, these plans directly contradicted the FBI's orders to stand down and only monitor the activity (Georgetown University, n.d.-b, para. 2; Georgetown University, n.d.-c, para. 3). Ackme has significant costs and resources at stake that are not tolerable for downtime, including its platforms and Historians for BSEE compliance (Georgetown University, n.d.-a, paras. 3, 9). Downtime costs for each platform could rise to over $300,000 each per day (Georgetown University, n.d.-a, paras. 3,9).

Vulnerabilities & ransomware impact on management and remote systems

Ackme has numerous vulnerabilities present that continue to expose itself to ransomware as well as other cyber threats:

1. Single Points of Failure: Ackme constructed a single point of failure by forcing recovery efforts to rely on only one server in its "server room" (Georgetown University, 2020, p. 9; Kirvan & Bigelow, 2021). In a ransomware situation where numerous hosts are under attack or seized, this is a poor recovery practice and a vulnerability in their recovery processes. Additionally, Ackme's remote administration system was only made for a single workstation with no known backups (Georgetown University, n.d.-a, para. 6). The compromise of these remote admin tools has completely hampered remote management and remote access to critical SCADA resources (Georgetown University, n.d.-a, para. 6). There are further references made to recovery issues throughout Ackme's incident response efforts, including the fact that any "system downtime" could result in interruption of key recovery processes (Georgetown University, n.d.-b, para. 2).

2. EOL (end of life) systems: Ackme has numerous end-of-life systems that were exploited by the attackers in the initial access of Ackme and have remained vulnerable through the exploitation and incident response process (Georgetown University, n.d.-b, para. 3). These systems do not even appear to have appropriate compensating controls to be properly implemented. Thus, it appears Ackme's cybersecurity and engineering teams are negligent in allowing EOL systems to be accessible and remain vulnerable. Only Ackme's EOL Windows systems were allegedly exploited during the attack (Georgetown University, n.d.-a, para. 5). These systems are also best described as highly important or business-critical in Ackme's offshore platform rig operations (Georgetown University, n.d.-a, para. 5).
3. Defensive security controls: There is no evidence that Ackme has deployed a comprehensive defense-in-depth strategy or any organized cybersecurity controls to defend its enterprise. We have no evidence of any detection or alerts triggering on Ackme's end to alert them of the intruder's presence, initial access, reconnaissance, lateral movement, persistence, or impact. Ackme appears to be a helpless victim at the mercy of the ransomware actor and the FBI.

BSEE compliance issues

Ackme has been risking BSEE (Bureau of Safety and Environmental Enforcement) compliance issues due to its poor recovery practices that were previously discussed which affect key BSEE-related hosts. Its Historians were compromised, which are key compliance and reporting hosts for Ackme's platforms (Georgetown University, n.d.-a, paras. 3, 9). This outage required cumbersome manual reporting, which may not be compliant for a BSEE inspection (Georgetown University, n.d., para. 3). BSEE can perform inspections spontaneously and without

advanced notice, surprising Ackme and requiring the sudden manual aggregation of required logs and data for compliance (BSEE, 2021, pp. 1-2). At the inspector's discretion, a facility could be completely shut down due to non-compliance with BSEE regulations and issue violations against Ackme as a license holder (BSEE, 2021, p. 2). Additionally, the FBI's instructions to only monitor and not respond to IOCs will further inhibit recovery efforts at affected platforms and augment BSEE non-compliance for Ackme.

Payload Analysis and IOCs

Ackme has considerable threat intelligence and indicators to work with in this incident thanks to the FBI (Georgetown University, n.d.-c, para. 3). While we know much of the initial access into Ackme occurred through EOL systems, Ackme's Badger AMR systems may have been the first traceable intrusion into Ackme via its supply chain (Georgetown University, n.d.-b, para. 2; Georgetown University, n.d.-d). This supply chain infiltration may have granted the adversary initial access into Ackme and provided ample opportunity for lateral movement to further compromise hosts, like Ackme's entire platforms. As far as the payload is concerned, we are not given this information. It is known that the ransomware is exploiting native cloud storage services to Ackme, like Amazon and Dropbox, to exfiltrate data (Georgetown University, n.d.-c, para. 2). This problem has allowed their exfiltration to be masqueraded by legitimate traffic. However, further IOCs (indicators of compromise) are provided, including outbound traffic to private range CnC (command-and-control) servers with exfiltration (Georgetown University, n.d.-c, para. 3). Exfiltration activities correlate with work hours within Russia and the threat actors switch between 6 different utilities (Georgetown University, n.d.-c, para. 3). The FBI has mentioned TLS activity is "of interest" (Georgetown University, n.d.-c, para. 3). Thus, Ackme

should seek to potentially use tools like TLS inspection via a web proxy in order to actually be able to inspect encrypted traffic (Google Cloud, 2023).

References

BSEE. (2021). Inspections Fact Sheet. In *bsee.gov*. Bureau of Safety and Environmental Enforcement. Retrieved September 16, 2023, from https://www.bsee.gov/sites/bsee.gov/files/fact-sheet//fnl-fact-sheet-bsee-inspections-5621.pdf

Georgetown University. (n.d.-a). *Module 3: In the Thick of a Ransomware Attack* [Slide show; Canvas]. Georgetown University Canvas. https://georgetown.instructure.com/courses/175977/pages/module-3-in-the-thick-of-a-ransomware-attack?module_item_id=3283361

Georgetown University. (n.d.-b). *Module 4: Do or Do Not* [Slide show]. Georgetown University Canvas. https://georgetown.instructure.com/courses/175977/pages/module-4-do-or-do-not?module_item_id=3283367

Georgetown University. (n.d.-c). *Module 5: FBI & DHS Get Involved* [Slide show; Canvas Online]. Georgetown University Canvas. https://georgetown.instructure.com/courses/175977/pages/module-5-fbi-and-dhs-get-involved?module_item_id=3283373

Georgetown University. (n.d.-d). *Module 2: Response to a Spear Phishing Attack* [Slide show]. Georgetown University Canvas.

https://georgetown.instructure.com/courses/175977/pages/module-2-response-to-a-spear-phishing-attack?module_item_id=3283355

Georgetown University. (2020). H. Ackme Oil & Gas Background Material. In *Google Drive*. Retrieved September 7, 2023, from https://drive.google.com/file/d/1TDoFQQWPZTgWTncVxTrKOfP2rMGkz_Re/view

IT Governance USA. (n.d.). *Data Breach Notification Laws by State | IT Governance USA*. itgovernanceusa.com. Retrieved September 28, 2023, from https://www.itgovernanceusa.com/data-breach-notification-laws

ISACA. (n.d.). *CMMI Institute - CMMI Levels of Capability and performance*. CMMI Institute. Retrieved September 28, 2023, from https://cmmiinstitute.com/learning/appraisals/levels

Kirvan, P., & Bigelow, S. J. (2021). single point of failure (SPOF). *Data Center*. https://www.techtarget.com/searchdatacenter/definition/Single-point-of-failure-SPOF

NIST. (2023). The Five Functions | NIST. *NIST*. https://nist.gov/cyberframework/online-learning/five-functions

SEC. (2023, July 26). *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*. sec.gov. Retrieved September 17, 2023, from https://www.sec.gov/news/press-release/2023-139

Taschler, S. (2023, August 9). *What is Cyber Threat Hunting? [Proactive Guide] - CrowdStrike*. crowdstrike.com. Retrieved September 28, 2023, from https://www.crowdstrike.com/cybersecurity-101/threat-hunting/

Thexpert, J. (2019, July 23). *Threat Briefing from Cyber Threat Analyst at Critical Infrastructure Co.* https://drive.google.com/file/d/1skFV5MPB6PqHuW8E239wrc5qP0PlEXUg/view?t=94s