Module 3: Vulnerability Assessment Report

Kyler Kent

School of Continuing Studies, Georgetown University

MPCR-7990-101: Capstone

Dr. Rosemarie Pelletier

September 17, 2023

Module 3: Vulnerability Assessment Report

This ransomware attack may significantly affect me as a private-sector CISO. As CISO of Ackme, this incident shows my potential failure in securing my organization against emerging cyber threats. The public will be scrutinizing my organization and my leadership as we file a Form 8-K per SEC rules to notify public shareholders of our cyber incident (SEC, 2023). We will likely face adverse media attention and demeaning interviews as we try to quickly recover from this incident. The private sector CTO of Ackme will likely face scrutiny once it is discovered that Ackme's critical IT systems are operating on Windows XP and systems have not been upgraded promptly. Additionally, the CEO could decide to invoke a board meeting and remove the CTO and CISO for the failures demonstrated in the ransomware attack. Finally, while we don't have evidence that there is impending legal, regulatory, or enforcement action against Ackme, the Legal/Regulatory Compliance Officer of Ackme is likely under significant stress to manage the legal aftermath of the incident for Ackme, its stakeholders, and shareholders. If BSEE intervenes and decides to shut down platforms, Ackme's Legal/Regulatory Compliance Officer could be removed due to lost compliance and licensing with BSEE by the CEO or the Board.

The private sector faces a unique victimization from a ransomware attack. While enduring the stresses of trying to maintain a prominent spot in a potentially competitive economic marketplace, private corporations must also adhere to an amalgamation of regulations and governance requirements for their organization. In the case of Ackme, they are a critical infrastructure oil and gas supplier and are subject to BSEE (Bureau of Safety and Environmental Enforcement) licensing requirements (BSEE, n.d.; Georgetown University, n.d., paras. 1,3). Specifically, Ackme suffered a compromise of "Historians" which are key components of Ackme's BSEE reporting requirements (Georgetown University, n.d., para. 3). Ackme operators report that data aggregation must now occur manually from individual hosts instead of from a central database (Georgetown University, n.d., para. 3). If BSEE decided to conduct an inspection, such as an unannounced “spot check” of an offshore rig, Ackme could be in serious trouble due to failure to produce necessary logs (BSEE, 2021, pp. 1-2). Penalties BSEE can levy include issuing an “Incident of Non-Compliance (INC),” which can “result in either a warning or a shut-in” (BSEE, 2021, p. 2). A “shut-in” can result in the closure of an “entire facility” (BSEE, 2021, p. 2). For Ackme, this could mean catastrophic financial losses by simply a surprise BSEE inspection at one of their facilities.

The government sector may face challenges in enforcing regulatory standards with Ackme. For one, BSEE enforcement may be hindered due to the failure of Ackme to produce necessary and timely reports (Georgetown University, n.d., para. 3). As a result, the BSEE may be unable to make an adequate compliance decision about Ackme. Additionally, the BSEE may be fearful of digitally interacting with the organization due to the ongoing ransomware attack. For example, the BSEE may restrict bringing portable laptops and tablet devices they normally issue to an Ackme site due to fear that Ackme’s ransomware could migrate to federal systems. This could significantly slow down an investigation and mandate the use of pen-and-paper documentation.

Vulnerabilities Found

People vulnerabilities

Ackme has many people vulnerabilities present within Ackme. Platform workers lack proper regulatory training and preparation for BSEE licensing requirements (Georgetown University, 2020, p. 9). If BSEE were to conduct a “spot check” at an Ackme facility or offshore rig, platform workers could poorly perform and put Ackme's BSEE licensing in jeopardy as well as potentially cause a location to close (BSEE, 2021, p. 2).

Additionally, Ackme workers were not given cybersecurity awareness or basic IT training for a cyber incident response (Georgetown University, 2020, p. 9). Ackme employees could be easily phished and used as an initial access vector for a ransomware threat actor. Next, in the event of the first indicators of compromise at Ackme for the actual ransomware attack on platform computers, Ackme employees would likely be clueless and disorganized. During the ransomware scenario, there is no evidence of any organized incident response by Ackme platform operators or Ackme's ARC or IT departments. There is no evidence of any organized communication strategy, such as a call list. Basic user awareness and incident response training could include signs of compromise and indicate it is time to call the IT security department and potentially disconnect computer systems from the network to prevent lateral movement, hence limiting the amount of damage the adversary can inflict on Ackme.

Ackme workers also lack the skills and capabilities to handle full-scale disasters, such as the "entire failure of the process computer system" (Georgetown University, 2020, p. 9). Thus, Ackme workers are not adequately prepared for a large-scale disaster, like a full-blown ransomware attack in the current capstone scenario.

Disaster recovery/configuration vulnerabilities

Ackme unfortunately decided to create a single point of failure in its recovery processes by making the "capability to restore all software" limited to "one of the servers in the server room" (Georgetown University, 2020, p. 9; Kirvan & Bigelow, 2021). Now, in the latest information we have in the scenario, Ackme has no backups available for the downed servers (Georgetown University, n.d., para. 4). This can likely be attributed to Ackme's frivolous disaster recovery practices and not implementing a proper backup strategy with multiple redundant backups necessary to support the continuity of a modern IT-dependent enterprise or organization (Posey, 2022). Furthermore, Ackme has unique configurations at each platform, appraising their local setups at each compromised location to be “approximately $2.5 million” (Georgetown University, n.d., para. 4).

Remote management systems were also poorly designed for Ackme in the event of an incident. Ackme designed apparently one remote access system via a “command line interface” with no failover, inhibiting the ability of the ARC to remotely monitor and administer the platforms and necessitate physical workers and presence (Georgetown University, n.d., para. 6).

High latency in recovery measures

Additionally, it appears no Ackme staff aboard platforms have any IT skills or support capabilities, forcing platforms to rely on remote incident response specialists (Georgetown University, 2020, p. 9). It could take up to 24 hours for Ackme to receive such specialists after an incident (Georgetown University, 2020, p. 9). Disasters, including cyber incidents, may require the immediate attention of a specialist. Most organizations today rely on high standards for continuity and availability, including the principles of “five 9’s” (Merker, 2020). Five 9’s means an organization is available and operational for 99.999% of a year, which equates to the downtime of about “5 minutes and 15 seconds in a year” (Merker, 2020, para. 1). Ackme would miserably fail these benchmarks with their current disaster recovery plan/setup. Ackme could incur at least $300,000 of losses daily at each offshore platform location if a disaster, cyber incident, or operational failure interrupted operations for a day (Georgetown University, n.d., para. 9). Additionally, Ackme maintains BSEE reporting requirements (Georgetown University, n.d., paras. 1, 3). Ackme’s reporting capabilities could be significantly degraded during a cyber incident as we have seen with the current ransomware attack and could result in BSEE adverse action (Georgetown University, n.d., paras. 1, 3).

Basic security controls

Ackme appears to lack basic security controls, such as a network firewall, host-based intrusion prevention systems (IPS), and, potentially, an SIEM. We have no evidence to date in the latest ransomware incident that Ackme has received any security alerting from the incident and the only indicators of compromise appear to be the ransomware note on compromised machines (Georgetown University, n.d., para. 2). Thus, Ackme appears to completely lack basic security controls that could detect, alert, and prevent an intrusion, including a ransomware attack. At the very least, security detection could have alerted potential lateral movement during the attack and prevented further hosts and platforms from being compromised.

Vulnerable hosts

Ackme appears to have a swathe of potentially vulnerable hosts on their platforms running “Windows XP,” a legacy and highly vulnerable version of Windows that Windows ended support in 2014 (University of Alaska Anchorage, n.d.; Georgetown University, n.d., para. 5). While Ackme claims it has only been able to upgrade a handful of hosts due to PLC compatibility issues, they were negligent by keeping their mission-critical systems (including HMI—human machine interface) on a highly vulnerable version of Windows (Georgetown University, n.d., para. 5). Ackme has hypothesized that the vulnerable Windows systems were the only ones exploited in the ransomware attack (Georgetown University, n.d., para. 5).

Poor supply chain and hardware lifecycle practices

In addition to the above vulnerabilities, there is evidence that Ackme has a poor supply chain and hardware lifecycle. Ackme has hardware “lead times up to 4 months” for new SCADA and platform systems (Georgetown University, n.d., para. 7). Ackme appears to be dependent on suppliers who are experiencing “backlogs” (Georgetown University, n.d., para. 7). The total time to upgrade all systems appears to be “3 years,” which is excessive considering Windows XP is a critically vulnerable operating system (Georgetown University, n.d., para. 7). These practices have left Ackme’s hosts vulnerable to exploitation just as they were in the ransomware attack, risking their continuity of operations as well as BSEE licensing due to affected reporting mechanisms (Georgetown University, n.d., paras. 1-7).

Vulnerabilities not potentially exploited

Poor IAM (Identity Access Management)

There is evidence that Ackme has poor offboarding procedures during the IAM lifecycle (Georgetown University, 2020, p. 10). Offboarding procedures have been described as “lax” and without stringent verifications and checks Georgetown University, 2020, p. 9). This could cause a major cyber incident, as a user who was offboarded could maintain access to Ackme information systems and sell access to a threat actor, such as a ransomware group for many thousands of dollars as an “initial access broker” (Freed, n.d.). Additionally, a terminated employee could wreak havoc as an insider if their account was not immediately disabled (Davis, 2022). These poor IAM procedures have also been a focal point during audits and could potentially lead to BSEE enforcement action against Ackme (Georgetown University, 2020, p. 10).

References

BSEE. (n.d.). *Oil & gas*. Bureau of Safety and Environmental Enforcement. Retrieved September 16, 2023, from https://www.bsee.gov/oil-gas

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

Davis, J. (2022, July 27). 75% of Insider Cyber Attacks are the Work of Disgruntled Ex-Employees: Report. *InformationWeek*. https://www.informationweek.com/security-and-risk-strategy/75-of-insider-cyber-attacks-are-the-work-of-disgruntled-ex-employees-report#

Freed, A. M. (n.d.). *How do initial access brokers enable ransomware attacks?* https://www.cybereason.com/blog/how-do-initial-access-brokers-enable-ransomware-attacks

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

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

Merker, K. (2020, June 15). *What is Five 9s Availability? Do you really need 99.999% Server Uptime?* https://www.nobl9.com/resources/do-you-really-need-five-nines

Posey, B. (2022). Craft a secure and reliable backup redundancy strategy. *Data Backup*. https://www.techtarget.com/searchdatabackup/tip/Designing-a-redundant-backup-solution

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

University of Alaska Anchorage. (n.d.). *Windows XP - End of Life*. Information Technology Services | University of Alaska Anchorage. Retrieved September 17, 2023, from https://www.uaa.alaska.edu/about/administrative-services/departments/information-technology-services/getting-help/knowledge-base/windows-xp-end-of-life.cshtml#:~:text=What%20is%20end%20of%20support,end%20on%20April%208%2C%202014.