Date: Oct. 11, 2022

To: CEO and Board of Directors of Berkshire Ontheball

From: Multra guard RESPOND Team:
Kyle Biery, Melvin Estrada, Mark Hunter, Sam Precie, Phuc Trinh

Subject: Analysis of Facility Response Measures and Recommendations for Improvements

Summary:

Repeating the Identify team's summary, the RESPOND team responded to the events of July 22nd, 2022 and examined potential responsive actions for similar attacks.

An overnight security guard with ties to the cyber underground and a hacker group that was hired by the client used their security access to open the way to the terminals controlling the facility's HVAC systems. They employed a password-cracking program and a botnet to render the HVAC systems inactive in order to cause a four hour network outage in which his group intended to launch a DDOS attack against a currently unknown target.

Incident Response Plan:

1. Examine active systems being affected by HVAC shutdown. Ensure that no permanent damage is done to the hardware.
2. Prepare off site backups
3. Reset Non-IT employee access (Passwords, Keycards, etc) and have active system admins standby to work on main servers. Have maintenance teams work on HVAC systems.
4. Terminate all inbound traffic to main servers and redirect to backup servers.
5. Monitor Backup servers for suspicious activity.
6. Temporarily restrict customer access to the site when transitioning back to main servers.
7. Verify all data is secure.
8. Monitor site for suspicious activity.

Future Improvements:

1. Implement automated switches to redirect traffic from overheated servers to cloud backups.
2. Utilize Gartner program to establish a Digital Forensics and Incident Response (DFIR) strategy.
    a. Forensic collection—gather, examine, and analyze data from networks, applications, data stores, and endpoints, both on-premises and in the cloud.
    b. Triage and investigation—determining the type of breach and identifying the root cause, scope, timeline, and impact of the incident.
    c. Notification and reporting— There will be notifications and reports on breaches sent to the compliance bodies. In addition, depending on the severity of the incident, there may be a need to notify authorities like the FBI and Cybersecurity and Infrastructure Security Agency (CISA) in the US.
    d. Incident follow up— Negotiate with attackers, communicate incident status to stakeholders, customers, and the press, and make changes to systems and processes to address vulnerabilities.

For further questions regarding the incident and our examination of the details, please contact Mark Hunter or Kyle Biery of Multra-Guard via our corporate email (multraguard@cybernet.com) or phone number (403-555-5555).