Multra-Guard

Oct. 4, 2022
To: CEO and Board of Directors of Berkshire Ontheball
From: Multra guard DETECT Team: Kyle Biery, Melvin Estrada, Mark Hunter, Sam Precie
Subject: Analysis of Facility Detection Measures and Recommendations for Improvements

Summary:

Repeating the Identify team's summary, the DETECT team investigated the observation and alert measures taken during and potential countermeasures for events similar to the night of July 22nd, 2022.

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.

Detection Methods:

Regarding the methods both existing and potential, the ways the client can go about detecting occurring cyberattacks are as such:

Physical:

-Existing:

Security Cameras: Allow for detection of suspicious activity from in-facility threats. Cameras around the affected room can recognize when the attackers have accessed the area under suspicious circumstances.

-Proposed:

Improved Security Patrols: Randomize Patrol Schedules to make it so that an additional security guard would be patrolling on a different schedule every hour so that the attacker would be caught off guard.

Motion Sensors: Place the sensors in key areas normally unoccupied in sensitive areas.

Timed Security Doors: Access to sensitive areas is on a timer in which the individual entering the room must enter a password within a time frame or confirm with the main security room that they have entered the area to grant access. Any other action results in an alert being sent to the security company.

Digital:

-Existing:

Virus Scanners : An antivirus software works by scanning incoming files or code that's being passed through your network traffic. Companies who build this software compile an extensive database of already known viruses and malware and teach the software how to detect, flag, and remove them.

Multi-Factor Authentication : Multifactor authentication combines two or more independent credentials: what the user knows, such as a password; what the user has, such as a security token; and what the user is, by using biometric verification methods.

-Proposed:

Security Tokens (MFA) - small hardware devices that store a user's personal information and are used to authenticate that person's identity electronically. The device may be a smart card, an embedded chip in an object, such as a Universal Serial Bus (USB) drive, or a wireless tag. A software-based security token application generates a single-use login PIN. Soft tokens are often used for mobile multi-factor authentication, in which the device itself -- such as a smartphone -- provides the possession factor authentication.

Security Access Software (CCure or Lennell) - Create a double access software that requires two personnel to accept access to the area before entering the location. Will alert area approver/manager of unauthorized access and will send alerts to on-call team to arrive on scene.

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).