Multra-Guard

Sept. 27, 2022
To: CEO and Board of Directors of Berkshire Ontheball
From: Multra guard PROTECT Team: Kyle Biery, Melvin Estrada, Mark Hunter, Sam Precie
Subject: Analysis of Facility Protective Measures and Recommendations for Improvements

Summary:

Repeating the Identify team's summary, the Protect team investigated the protective 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.

Countermeasures:

There are numerous countermeasures that exist here and can be implemented to protect against such attackers in the future.

Physical:

Existing:

Door Locks: Rendered moot by the Security Guard's possession of the keycard needed to gain access to the maintenance areas. Recommend against restricting access to areas in the event of fires.

Proposed:

Machine locks: Restrict terminal access via physical covers over the terminals accessible to system techs with emergency shut offs available to general personnel in the event of fire or other emergencies.

Digital:

Existing:

Remote Management and Threat Mitigation system: Allowed for system admins to be alerted to the changes the guard made and respond relatively quickly, keeping the outage to a four hour window.

Proposed:

1. **Virus Scanner -** Total AV, PCProtect, Scan Guard, Bitefender, Norton, AVG, Avast, McAfee. Malwarebytes, BullGuard, Kaspersky, ESET, Panda, Trend Micro, F-Secure
2. **Secure Shell (SSH) -** SSH Clients, PuTTY, Tectia for IBM, WinSCP, CyberDuck, Tectia, BothanSpy
3. **Two-Factor Authentication -** Microsoft Authenticator, Google Authenticator, Duo Security, LastPass, Authy, Okta MFA VPN, RSA SecureID, Ping Identity, OneLogin, WatchGuard AuthPoint, Auth0, Uniqkey
4. **24 Hour Automatic Backups** - Backblaze, Carbonite, NAKIVO, PcCLoud, PolarBackup, LiveDrive, iBackup, Cyber Backup, Genie9, AOMEI

Countermeasure Maintenance:

1. Antivirus programs can use one or more techniques to check files and applications for viruses. While virus programs didn't exist as a concept until 1984, they are now a persistent and perennial problem, which makes maintaining antivirus software a requirement. These programs use a variety of techniques to scan and detect viruses, including signature scanning, heuristic scanning, integrity checks, and activity blocking.
2. SSH is a secure application layer program with different security capabilities than FTP and Telnet. Like the two aforementioned programs, SSH allows users to remotely log into computers and access and move files. The design of SSH means that no cleartext usernames/passwords can be sent across the wire. All of the information flowing between the client and the server is encrypted, which means network security is greatly enhanced. Packets can still be sniffed but the information within the packets is encrypted.
3. Two-Factor Authentication (2FA) works by adding an additional layer of security to your online accounts. It requires an additional login credential – beyond just the username and password – to gain account access, and getting that second credential requires access to something that belongs to you. To alleviate anyone from having access to negatively affect the organization, the Two-Factor Authentication will alert the direct manager and route access through two employees instead of one.
4. IT Automation is a process of automating jobs, batch processes, and workflows across IT. It includes a wide variety of tools, practices, and capabilities. It can be used for a variety of use cases. It is a quickly evolving field and incorporates new technologies like machine learning and artificial intelligence. These tools are created to integrate automatic

security processes that monitor employees actions throughout the network. A daily completion of batch processes are used with internal and external firewalls to increase efficiency and execute support for any security breaches.

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).