Cyber Juice

Frank Baumgartner, Jackson Wilhite, Trennan Lilly, Nicholas Lauro
Computer Science and Information Technology
Advisor: Professor David Corcoran

Introduction

- Cybersecurity-focused project
- Objective was to provide recommendations for local water utility plants
- Interviewed clients, performed in-person visits, and gathered as much documentation as possible.
- Developed plans that provided ways for the clients to increase their cybersecurity
- General policies and technology, as well as site-specific fixes

Methodology

- Interview water superintendent
  - Gather as much information as possible
  - Get contacts for managed service providers
  - Receive documentation for configurations
- Analyze collected data
  - Pay attention for online SCADA interface
  - Identify weak policies/procedures
  - Search for vulnerabilities related to programs/services
- Develop recommendations
  - Peer reviewed by professionals
  - Compile in a document and review with clients
- DID NOT PERFORM SCANS
  - We are NOT PROFESSIONALS
  - Did not want to break delicate systems
  - Recommended using CISA for deeper scans

Team

Frank Baumgartner

Nicholas Lauro

Trennan Lilly

Jackson Wilhite

Important Areas

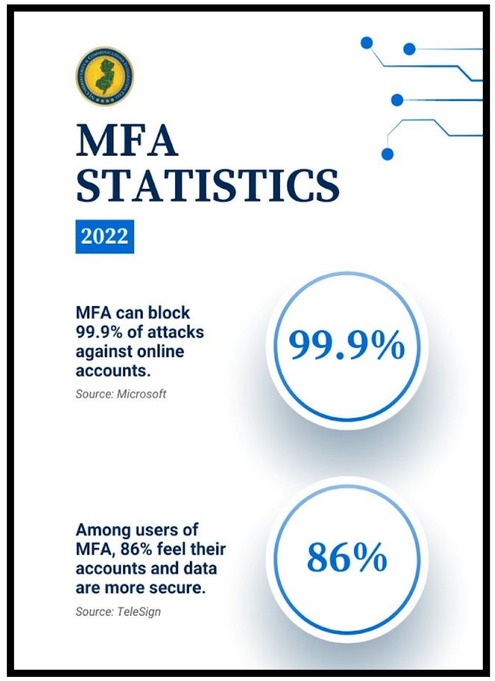
SCADA

- Supervisory Control and Data Acquisition
- A system that combines hardware and software components that allows clients to gather real-time data on water pressure, tower leves, pumps, etc.

Multi-Factor Authentication

- MFA for short, which requires an additional knowledge token for authentication
  - Code, passphrase, or more sent to phone/email
- Helps increase account security and prevents attackers from logging into technologies
- 99% of account attacks are prevented by MFA

Statistics



Important Areas

Email

- Phishing emails make up 36% of all data breaches
- Many email providers, such as Outlook, has specific settings/technologies that can be configured that can prevent phishing attacks

User Policies

- Simple user actions, such as logging out of computers or the storage/usage of credentials, can be the difference between having a secure network and being hacked
- Regular user training better implements these policies and reduces user related breaches

Conclusion

- Our clients are now equipped with the essential technologies and procedures to strengthen their cybersecurity posture
- They have a clear understanding of the daily practices they should follow to better protect their devices and the data
- Our contacts now possess the policies and tools needed to effectively implement new technologies and system updates

Logo

Contacts

jacksonwilhite1@gmail.com

trennanlilly@gmail.com

xbaum1@outlook.com

nicholaslauro2003@gmail.com