Schuyler County Ransomware Attack: Lessons Learned

Incident Overview

- August 30, 2017 – Schuyler County suffered a cyber attack affecting all County servers and programs.
- Attack began between 8/13 and 8/21 via "brute force" attempts to penetrate system.
- 8/21- Successful log-in from an internal server via a standard user account.
- 8/30- After network reconnaissance, attacker elevated privileges to administrator account with weak credentials. Access from the administrator account was used to enumerate the domain, create test files across server and workstation assets, and ultimately deploy and execute a malicious binary code that encrypted files.
- Over the course of next few hours, county systems continued to become unavailable as the encryption of files spread throughout the network ultimately infecting all county departments.

Incident Overview

- County Background / Demographics
- County – BOCES Partnership
- Response by NYS CYCOM
  - Onsite analysis and triage
  - Traced likely ingress vector and path of infection
  - Collected malware binary samples and directed cloning of virtual servers for transport back to Albany forensic analysis lab.
  - Found no evidence of data exfiltration
- Role/Response FBI
  - Special Agent Ken Jensen
- Initial Priorities
- Teamwork & Partnerships

Key Findings: Situational Assessment

- **Observation 1 – (Strength)** Numerous departments noted that the immediate response to assuring continuation of services to clients, was delivered largely due to resiliency of individual employee efforts.
- **Analysis** – Most department mangers noted that as the ransomware attack evolved and the magnitude expanded, it was the quick and efficient efforts of departmental staff to revert to back-up methods (IE. Pen, paper, printed forms, etc.) that allowed essential services to continue to be delivered to clientele.
- **Observation 2 – (Opportunity for Improvement)** During the time immediately following the ransomware attack (Day 1 thru Day 4), communication of vital information to staff, was problematic or deficient due to loss of the e-mail server.
- **Analysis** –The initial aftermath of the ransomware attack proved challenging as the loss of the countywide e-mail servers created a lack of situational awareness amongst department managers due to the limited ability of disseminating relevant incident information

Key Findings: Information Sharing

- **Observation 3 – (Opportunity for Improvement)** Communications with clients and external partner agencies was extremely hindered due to lack of access to contact information and further essential data on main servers.
- **Analysis** – Due to most departments having schedules, client contact information, and associated case information stored on the main computer servers, staff found it very difficult to reconstruct this information until IT services were restored approximately 4 days after initial attack.

Key Findings: Cybersecurity

- **Observation 4 - (Strength)** 911 phone services and emergency services radio communications remained functional due to being independent from other county networks.
- **Analysis** – 911 telephone services and first responder radio systems, remained functional due to their existence on an autonomous network.
- **Observation 5 - (Opportunity for improvement)** – Schuyler County 911 Center “Computer Aided Dispatch” (“CAD”) services, recorder services and mapping services were incapacitated by the ransomware attack.
- **Analysis** – Although 911 services and radio communication were never compromised, certain aspects, such as “CAD” service, mapping services and voice recording were incapacitated.

Key Findings: Cybersecurity

- **Observation 6 - (strength)** Staff with non-critical roles redeployed to support departments with more critical needs.
- **Analysis** – Staff from departments with non-essential or limited critical services to provide (ie. Planning, County Legislature, etc.), assisted in other departments that needed assistance with delivering essential services.
- **Observation 7 - (Opportunity for Improvement)** During the restoration of servers, IT staff became overwhelmed with various departments requesting restoration of services.
- **Analysis** – As IT services were being re-established, IT staff found it very difficult to handle requests for prioritized department and service restoration.

Key Findings: Cybersecurity

- **Observation 8 - (Opportunity for Improvement)** Encrypted files and/or data saved to affected individual devices (flash drives, desktop folders etc) were unable to be restored.
- **Analysis** – Staff from several departments noted that documents and information saved to an individual device (Desktop, flash drive), were lost and unsalvageable by IT staff.
- **Observation 9 - (Opportunity for Improvement)** IT security detection and prevention devices were insufficient to distinguish and prevent the ransomware attack.
- **Analysis** – Intrusion detection systems and devices in place at the time of the attack were inadequate to prevent the style of attack that occurred on August 30, 2017.

Lessons Learned

- **Recommendation 2.1** - Schuyler County should explore options to relay vital incident related information to all county offices/buildings in the event of an emergency. Options may include a county wide phone paging system and should include a redundant back-up in the event one system becomes disabled.
- **Recommendation 2.2** - Schuyler County Administration and Department Managers should enact a policy for pre-establish "Emergency Purchases" to allow for continuance of essential functions such as operation of the jail, OFA meals, etc.
- **Recommendation 3.1** - County Departments should research and implement "Low-Tech" back-up options for essential documents, client contact information, vital phone numbers, and phone systems.

Lessons Learned (cont)

- **Recommendation 3.2** - County Departments should study and implement "Cloud Based" or "Flash Drive" based electronic back up services, for vital client information. Where applicable, departments should explore redundancy options with state agency systems for client scheduling, contact information, etc.
- **Recommendation 3.3** – Schuyler County should consider placing fax machines in each county owned or operated building to allow for internal and external communications should an interruption of IT services occur.
- **Recommendation 5.1** - Schuyler County Emergency Management should research and implement an internet based or some other independent back-up system for 911 "CAD", mapping and recorder services.

Lessons Learned (cont)

- **Recommendation 7.1** - Develop guidelines for prioritization order of re-establishing essential and critical services. Although priorities will be dictated by the magnitude and specifics of an event, guidelines should be established to prioritize the recovery order of the critical services. (IE:)
- o 911 service
- o Building HVAC systems
- o Security/access controls
- o Fuel access/shared fuel facility
- o Payroll services (ADP)
- o Accounts payable/receivable (KVS)
- o Subsistence Financial Services essential to Clients
- **Recommendation 7.2** - Schuyler County departments should establish an "IT Point Person" to assist with IT issues and serve as a point of contact for county IT staff.

I.T. Actions/Recommendations

- **Recommendation 9.1** - Schuyler County IT services should institute additional security considerations and recommendations including intrusion detection and prevention devices, syslog / centralized logging, and the addition of a correlation engine such as SIM or SIEM technologies.
- **Recommendation 9.2** - Schuyler County IT servers should be subjected to regular vulnerability scanning of externally available devices and implementing a patch management plan.
- **Recommendation 9.3** - Schuyler County should implement policies and procedures imposing all external access to the county network, subject to a 2-step verification and authentication process.
- **Recommendation 9.4** - Although already in place at the time of the August 30, 2017 incident, Schuyler County should review current insurance policies and assess the benefit of additional comprehensive cyber insurance.

I.T. Changes As A Result Of Attack

- Recovery has strengthened overall operation
- In-depth auditing of all user accounts. The use of generic accounts is very limited and is application specific.
- Generic accounts have limited login ability
- Division of duties across administrative accounts
- Standard user accounts have no admin privileges
- Granular password and maximum password age policies
- All user accounts have access to only the resources they need through the use of access control lists (ACL)
- Segmentation of network to minimize potential attack surfaces using VLAN's and ACL's
- 2-step verification required for all remote connections to the county
- Reduced the number of public facing resources
- Multiple backups of all servers stored off-site (outside of the county)
- Implementation of failover technology to increase uptime of all servers
- Migration to Office 365 for email