Staying Out of the Headlines

Cybersecurity Must-Haves So Your City Is Protected and Out of the News

Joe Howland, VC3

Chief Information Security Officer

VC3

ASSESS • IMPROVE • MANAGE

Cities That Didn't Stay Out of the Headlines

- **Whistler, British Columbia (April 29, 2021)**: "Whistler resort municipality hit by new ransomware operation" (Source: Bleeping Computer)
- **Oldsmar, Florida (February 8, 2021):** "'Dangerous Stuff': Hackers Tried to Poison Water Supply of Florida Town" (Source: New York Times)
- **Hafnium Attacks (March 8, 2021)**: "Microsoft Exchange Server attack hits local governments" (Source: GCN.com)
- **Colonial Pipeline (May 8, 2021)**: "Cyber-Attack Shuts Colonial Pipeline" (Source: Bloomberg)

It Could Happen to You

95% of all successful attacks over the past two years started in email.

The Traditional Attack

- **Direct Hacking**
  - Attempting to penetrate an organizations firewall
  - Attacking known vulnerable code in applications
- **Denial of Service (DoS, DDoS)**
  - Flooding an organization with data to prevent legitimate business
- **Man-in-the-Middle Attacks**
  - Listening in on a protected “conversation”

Evolving Threats

- **Ransomware –** The ability to quickly monetize a successful attack
  - **….. enhanced by black mail –** Using stolen data to try and force ransom payouts
- **Credential theft –** Dramatic rise in phishing emails designed to capture user credentials
  - Compromised mailboxes
- **Fraudulent Wire Transfers –** Higher risk for public entities

Evolving Threats

Cyber-attackers that breach your systems stay inside an average of over 200 days.

What are they doing?

- Spreading laterally across your network
- Looking for protected data to harvest– Personally Identifiable Information (PII), Credit Cards, etc.
- Trying to elevate privileges
- Concocting ways to disable anti-virus
- Attacking your backups

Cyber Liability Insurance

Premiums are going up as cyberattacks increase and become more financially damaging.

- Direct written premium growth increased over 22% in 2020
  - Renewals being declined if adequate security measures are not in place
- Cyber liability insurance providers wary of increased cybersecurity risks due to remote work
- Cyber liability insurance remains incredibly valuable—but premiums can be lessened with cybersecurity best practices

Security Management Framework

National Institute of Standards and Technology
https://www.nist.gov/cyberframework

Identify

Document what you need to protect and where it is located.

- ❑ An accurate asset inventory
- ❑ Where is your protected data?
- ❑ Cloud providers: What security is included and who is responsible for setting it up?
- ❑ What are your regulatory or compliance requirements?
- ❑ Supply chain – Which vendors would impact you if they are compromised?

Protect

Solutions to proactively identify weaknesses in your IT infrastructure and alert your city to security-related issues.

- ❑ Employee Policies and Training
- ❑ Two-factor Authentication (Not email based!)
- ❑ Anti-virus
- ❑ Spam Filtering
- ❑ Malware Protection
- ❑ Data Loss Prevention
- ❑ Patch Management
- ❑ IPS (Intrusion Prevention Services)
- ❑ Change Control Policies and Procedures that consider security
- ❑ Mobile Device Management
- ❑ Web Content Filtering

Detect

Technologies used to detect suspicious network traffic or behavior.

- **MDR / EDR (Managed Detection and Response / Endpoint Detection and Response)**: Security professionals watching your network and your endpoints (servers, computers, mobile devices, etc.) to monitor for threats.
- **Regular Security Scans**: Find security holes in your systems before someone else does.
- **Dark Web Monitoring**: Identify stolen and breached accounts sold on the black market.
- **Next Generation Firewalls:** Move from passive to active protection
  - **W/ IDS (Intrusion Detection Services)**: Watch for suspicious network traffic.
- **SIEM (Security Information and Event Management)**: Sift through the many security alerts received from different systems to identify the most important and critical. (May be included with MDR)

Respond / Recover

Solutions and processes that help mitigate the impact of a security incident.

- ❑ Offsite Log Retention – Used for evidence related to cyber incidents
- ❑ Incident Response Plan – How will you respond to a cyber event?
- ❑ Cyber Liability Insurance – Financial protection in case of a cyber event.
- ❑ Data Backups – Onsite, Offsite, Testing
- ❑ Business Continuity Plan

Overall Security Checklist

- **Protection**
  - ❑ Antivirus
  - ❑ Spam Filtering
  - ❑ Malware Protection
  - ❑ Data Loss Prevention
  - ❑ Patch Management
  - ❑ IPS (Intrusion Prevention Services)
  - ❑ User Policies and User Training
  - ❑ Change Control Policies and Procedures
  - ❑ Two-factor Authentication
  - ❑ Mobile Device Management
  - ❑ Web Filtering

- **Detection**
  - ❑ MDR / EDR
  - ❑ IDS (Intrusion Detection Services)
  - ❑ SIEM (Security Incident and Event Management)
  - ❑ Regular Security Scans
  - ❑ Dark Web Monitoring

- **Response / Recover**
  - ❑ Rock Solid Data Backup
  - ❑ Offsite Log Retention
  - ❑ Incident Response Plan
  - ❑ Cyber Liability Insurance

What If I'm Attacked?

You need a Cybersecurity Incident Response Plan that includes:

- A cyber insurance carrier
- An IT team or provider
- A partnership with law enforcement
  - Local Law Enforcement
  - FBI Internet Crime Complaint Center (IC3) (https://www.ic3.gov/)

Click cautious > click curious

Thank you!