PROTECTING YOUR BUSINESS FROM ITS' BIGGEST THREAT: CYBERATTACK

Allied Alloys

OUR STORY

- How?
  - Early morning on March 8, 2020 our IT company discovered “threat actors” had compromised our management system provider’s (MSP) data center network and over the course of a few weeks managed to gather intel on all of the MSP’s clients.
    - This was the day *before* Covid-19 was announced here in the USA.
  - Attackers removed antivirus software and began encrypting the MSP’s backup system.
  - They then deployed ransomware to encrypt all client’s data in the data center and locally at client sites via existing VPN affecting user’s workstations.
  - That same morning, MSP had contacted the attackers and received a ransom note for $800,000 in crypto currency payments to return close to 6 months of data, documents, and files that were encrypted (stolen).

- Where are we now?
  - It took us over a month to rebuild the 6 months worth of data that was taken.
  - We immediately moved our IT management services over to another MSP.
  - The former MSP hired a 3rd party digital forensics company to further explore this matter.
  - A formal investigation was opened with the FBI however to this date there is no definitive answer to how the attackers gained access to the entire MSP’s system. It is believed that a domain admin level account was compromised either via malicious email link or tech application vulnerabilities.

WHAT CAN YOU DO?

- Get the right insurance coverage
- Train your employees
- Add email warning notifications
- Include web filtering
- Anti-virus scheduled scans
- Move to cloud-based servers/hosts
- Multi-factor authentication

INSURANCE COVERAGE

- Ask your insurance broker or carrier for a full liability coverage of at least $1M
- What should this include?
  - A network, this is where the real benefit lies. One phone call and you should be provided with
    - Legal experts
    - A forensics team
    - Experts in ransomware attacks
  - 3rd party claims such as:
    - Business interruption
    - Rebuilt of your network/servers
    - Ransomware payout

EMPLOYEE TRAINING

- Training employees on how to identify potential threats by examining email content more thoroughly.
  - Matching the sender's Display name against the email address.
  - Hover over links to check URL/web address
  - Check for broken English

EMAIL WARNING NOTIFICATIONS

- Ask your IT department to add warning text to all emails that originate outside of the organization.
  - Helps protect against email spoofing by notifying the recipient that the message did not originate internally.

COMPANY-WIDE WEB FILTERING

- Enabling web filtering helps to protect users from accessing potentially malicious sites.
  - If user was not able to correctly identify malicious email and clicks on link, this would be an added measure of security to help block the site.
  - You can also now do this with company issued cell phone
    - MDM through Apple/Verizon

ANTIVIRUS SOFTWARE

- If employee training and web filtering fails, local antivirus solutions would be the next step in preventing a malicious attack.
  - Scheduled and on-demand scanning can help stop an attack before it happens and keep the threat local before it spreads to other endpoints on the network.

MICROSOFT 365

- Start moving to a cloud host
  - Microsoft OneDrive and SharePoint feature ransomware detection, notification and recovery options in the event that an attack does occur.
  - Makes restoring files possible and easier than before.

MULTIFACTOR AUTHENTICATION

- Enabling MFA can help prevent user accounts from being compromised.
  - Double verification for wires and bank details.