CASS

01

Cyber Security

Presented by Edward B. Kangeter IV

02

Topics

1. The Problem
2. How The Virus Entered
3. Repercussion & Ramifications
4. Cost & Downtime
5. Actions to Correct the Problem
6. Highlights

The Problem

How Was it Identified?

- CASS users reported an email issue.
- IT discovered files & folders were being encrypted one by one.
- IT was forced to shut down all devices & business-critical applications to avoid further encryption.

Encryption

- The method by which information is converted into secret code that hides the information's true meaning.

How the Virus Entered

What Happened?

- CASS employee received an email with an attached invoice.
- When the employee opened the invoice, the **EMOTET** virus was downloaded onto their computer and entered our network.
- The virus activated itself after a period of time and spread using shared drives on the network.
- The virus downloaded an encryption **TRICKBOT** which hides in the network and was not detected by any virus or malware scanners.

How the Virus Entered

EMOTET

- Malware program that was originally developed to access foreign devices and spy on sensitive & private, banking data. Emotet has been known to deceive basic antivirus programs and hide from them. Once infected, the malware spreads & infiltrates other computers in the network.

TRICKBOT

- Malware spread primarily by emails that contain malicious attachments or links.

Repercussions & Ramifications

The Following Became Encrypted

- Accounting Server
- Archive Server
- Backup Server & Historical Data
- ERP (Enterprise Resource Planning) Software
- Finance Servers

Consequences

- **6 months** of financial data was encrypted and had to be re-entered manually.
- As of today, there is data that we are unable to locate or recover.

Cost & Downtime

IT Related Costs

- $100,000+ to recreate servers & reinstate operations
  - IT Team worked 18 hour days for 7 days straight to reinstate CASS servers
  - 600+ hours to restore CASS to full operations

Accounting Related Costs

- $100,000+ to recreate encrypted financial data

Actions to Correct the Problem

Firewall

- Network security device that monitors & filters incoming and outgoing network traffic based on an organization's previously established security policies.

CASS Security Advantage

- Advanced Malware Filters provided by Cisco
  - Content filtering undesirable web content
  - Intrusion Detection & Prevention

Actions to Correct the Problem

DNS (Domain Name System)

- Translates readable domain names (eg. www.customalloy.com) to machine readable IP addresses (eg. 192.0.2.44).

CASS Security Advantage

- Block malicious sources before a connection is ever established.
  - Cloud Applications
  - IP Addresses
  - Unwanted Domains

Actions to Correct the Problem

CASS E-Mail Security Advantage

- Browser Isolation
  - Isolates the user's browsing activity, eliminating the opportunity for malware to access their device or network.
- Email Attachment Sanitization
  - Strip all Word, Excel, Powerpoint, HTML files from emails
  - Users must contact IT for any stripped documents
  - IT manually screens documents before releasing to users
- Impersonation Protection
  - Detects emails that pretend to come from well-known brands or from people within the organization
- Website Link Protection

Actions to Correct the Problem

CASS Endpoint Protection Advantage

- Two-Factor Authentication
- Artificial Intelligence virus scanning & remediation
- Complex Passwords
  - Letters
  - Numbers
  - Symbols
- Firewall enabled only for known business applications
- Meraki Mobile Device Management
  - Secure connection between mobile device applications and critical business servers
- Upgrade all PCs & Servers to latest OS & patch on a weekly basis

Actions to Correct the Problem

CASS Backups & Replication Advantage

- Backup Server & Storage is on its own virtual network which is hidden from PC's & Servers within our network.
- Replicate 1 month of backup data to secure, off-site storage

Actions to Correct the Problem

CASS Wireless Network Security Advantage

- Security policy only allows device with security certificate to connect to the CASS Wireless Network.
- Separate Network for Guests to only allow access to internet.
- Wireless Networks are set not to broadcast to the public.

Recommendations

- Hire a professional, third-party to audit your existing cyber security system.
- Implement a robust cyber security solution to help prevent & detect breaches.
- Have a plan in place with IT on steps to take in case of breach.
- Organizations should have their backup data separate from their network.
  - Recommended: Minimum 1 Month of Backups to be completed offsite.
- Purchase appropriate insurance for cyber security breach.

Contact Us

For questions or comments

Phone Number

510.893.6476

Email Address

edward@customalloy.com

Website

www.customalloy.com