Brick Township
Municipal Utilities Authority

Getting Hacked

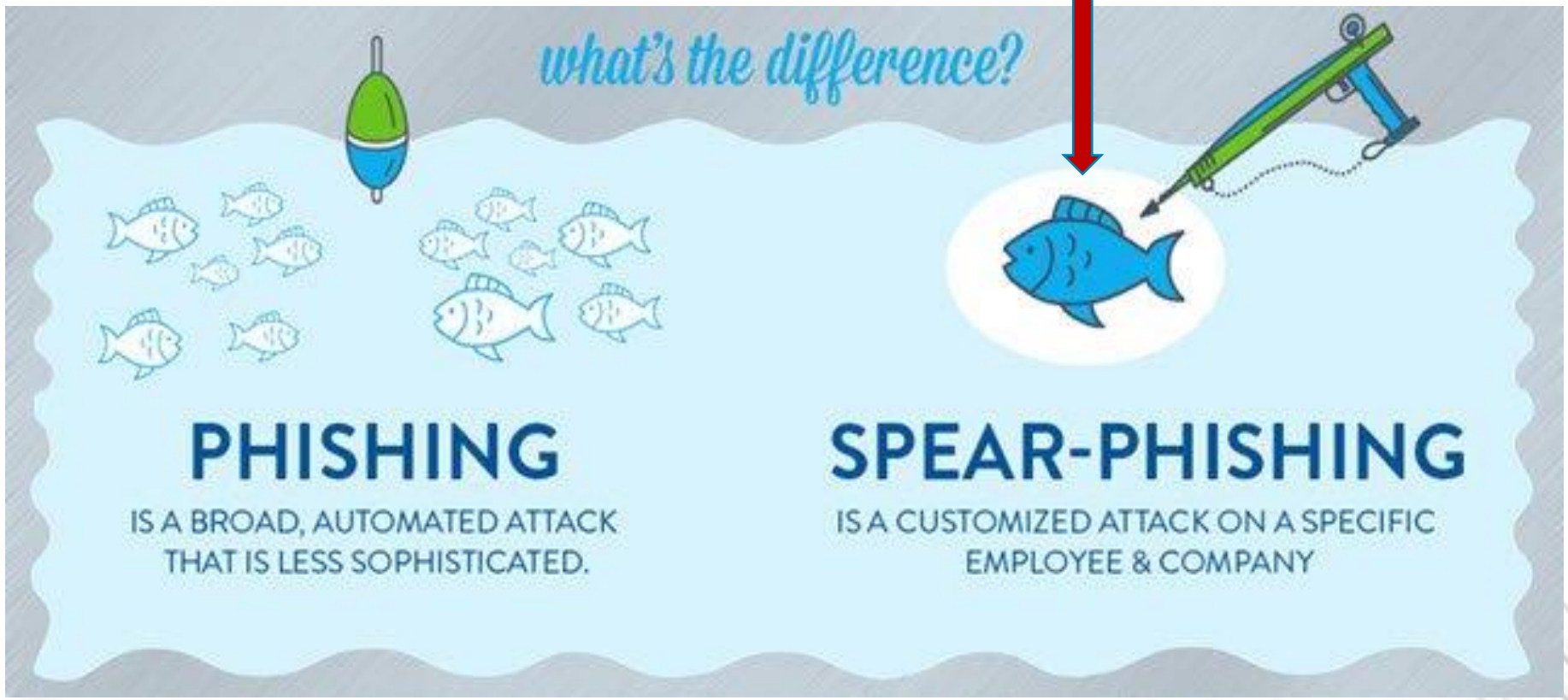
Presented by:
Janice Zelnock, CGCIO

BTMUA Cyber Incident

1. Events leading to cyber attack
2. Informing officials/employees
3. Keeping critical business functions running
4. Virus containment and remediation

Day 1 - Spear Phishing

User opened suspicious email with ‘Invoice.doc’ attachment



Day 2 – Cyber Fraud

- **Unauthorized charges**
  Employee Amazon accounts

- **Unauthorized charges**
  BTMUA Staples account

- **Thousands of emails**
  sent to Finance computer

Day 2 – Get Assistance

McAfee Support

"Total Endpoint Threat Protection" - Identified '*Artemis*' virus

How to we clean/remediate?

Multi-State Information Sharing & Analysis Center (MS-ISAC)

Advice on cyber threat prevention, protection, response, recovery

Confirmed we are infected with **Emotet** trojan

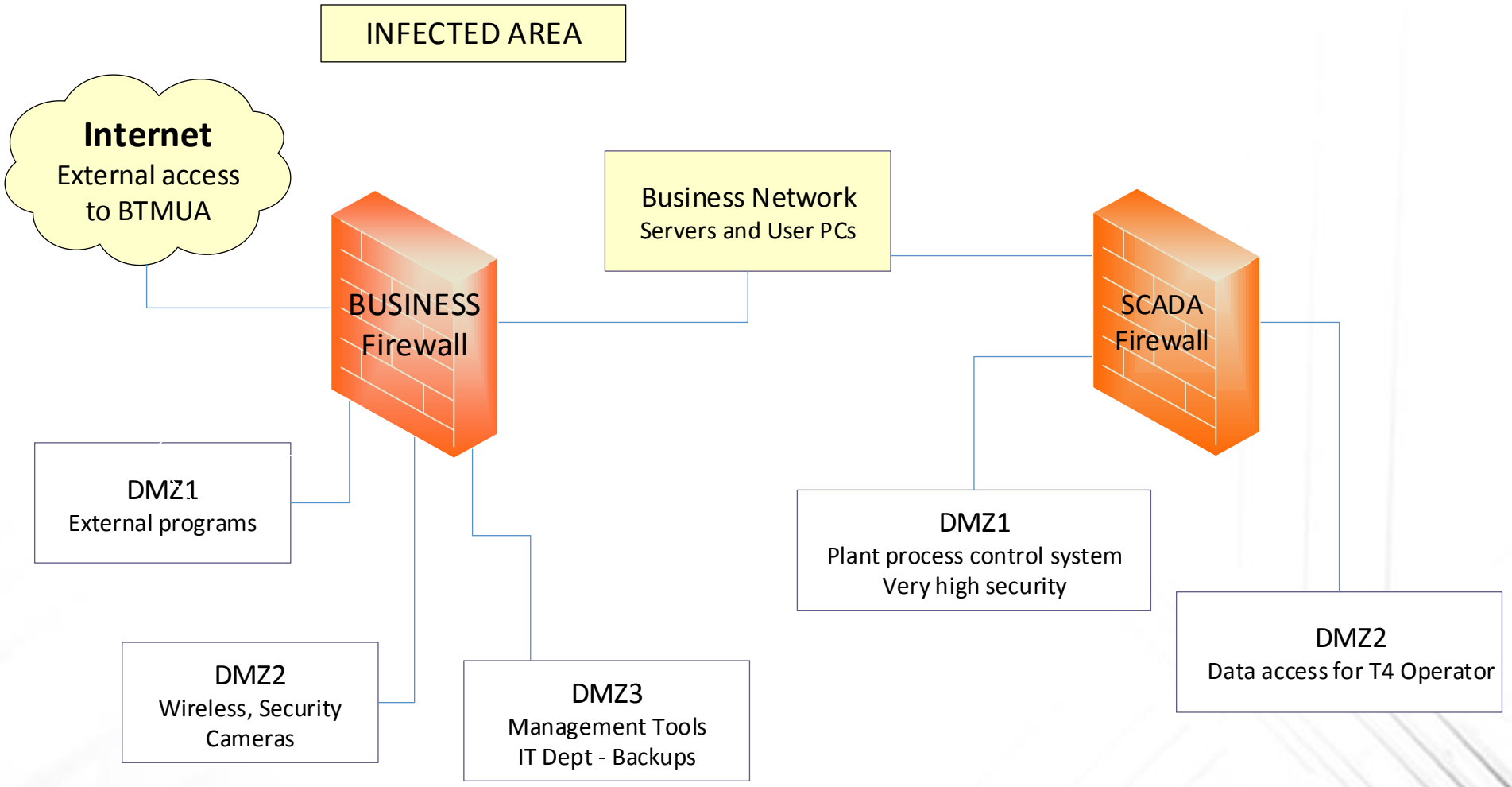
Day 2 – Emotet

Most anti-virus programs do not detect Emotet

- Steals network usernames & passwords

- Steals outlook email contacts
- Steals confidential account credentials used for online payments and banking systems.
  - Credit card info used for online shopping (Amazon, Macys, Etsy, Staples)
  - Banking logon info (PNC, TD, CitiBank)

Day 2 – Scope of Infection



Day 2 - Black Friday

- Emotet is not cleanable
- Hackers in system now
- Shut down network now
- All infected Servers and PCs
  - Restore from backup

    or
  - Wipe clean (reload)

Day 3 – Scope of Infection

Devices

- 26 File Servers
- 120 user PCs

Day 3 – Scope of Infection

Programs

- Email, Excel, Word
- Finance, Billing
- LIMS (Laboratory Information Management system)
- **WIMS** (Water Information Management System)
- **Payroll**

Day 3 – No breach of PII data

SQL Databases

- Personal Identity Information (PII)
- Customer data
- Financial data
- LIMS, WIMS data

Day 4 – Critical Functions

Payroll

Everyone needs to get paid

WIMS

T4 Operator of Record must file monthly reports with DEP

Days 3-4 - Inform Officials/Executive Staff

Conference Call

- Network will be down upcoming week
- Estimated time frame to recover
- Critical Business functions up first

  Payroll, Plant reporting (WIMS)

Day 4 *"Boots on the ground"*

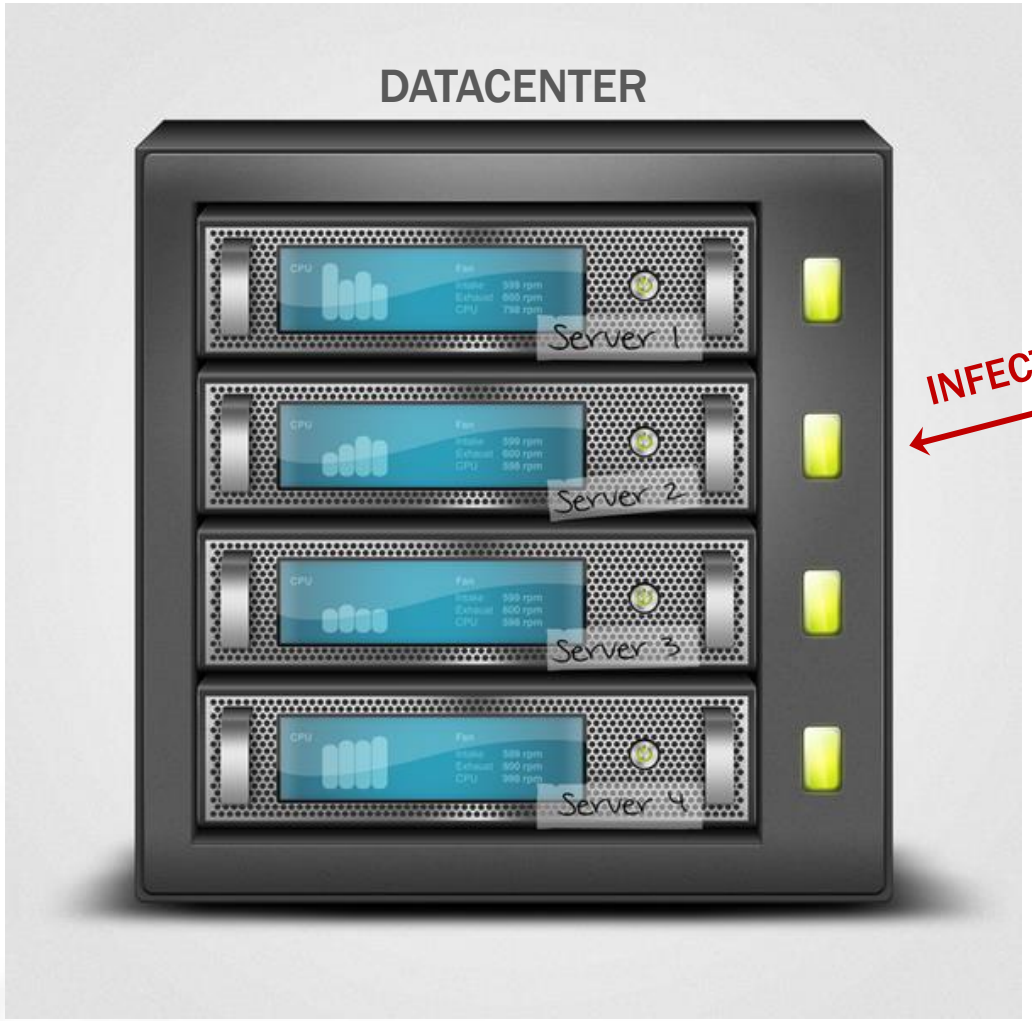
NJCCIC

New Jersey Cybersecurity and Communications Integration Cell

- Provide a team of trained network administrators
- Identified infected PCs
- Reload infected PCs

Day 5 - NJCCIC

Day 5 – Get Everyone Paid



INFECTED NETWORK

Day 5 – Passwords

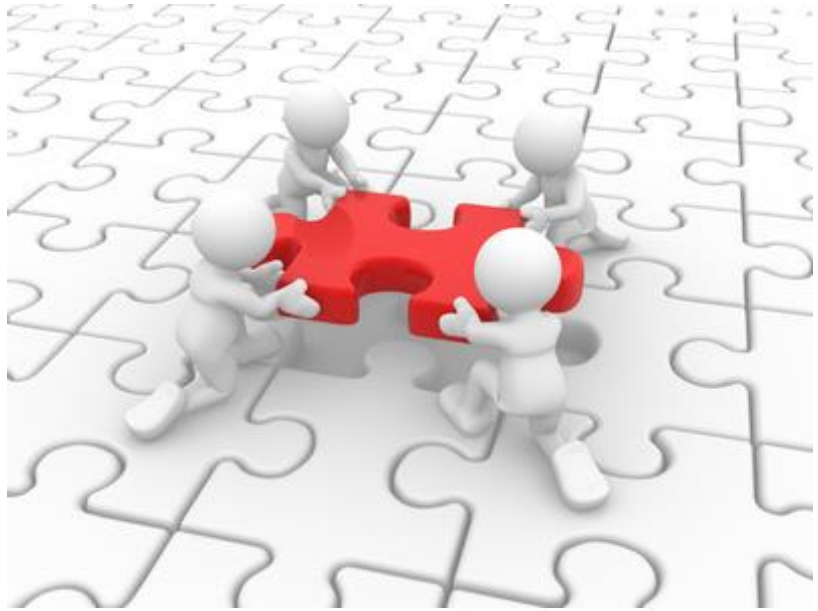
- BTMUA network

  Force new password at next logon

- Change personal passwords for accounts accessed at work

  Order status, Banking, Credit card

Days 5-10 Remediation



Team IT

Restored Servers using backups before Emotet infection

Team NJCCIC

Restored / Reloaded infected user PCs

Days 5–10
How do we stop this from happening again?

Prevention/Containment

- VLANs – Split the network into smaller sections
- Limit user ability to make changes to PC
- User awareness training

Weeks 1 – 4 Getting Users back on the Network

Team IT

- Added users one at a time
- Setup VLANs on the network
- Added each user to assigned VLAN

BTMUA employee downtime
10 days – 4 weeks

Week 5 - User Awareness Training

Will I be the next person to click on an email containing a virus?

- In person staff training

  Review of Emotet, cyber awareness session, how to identify malicious email

- KnowBe4

  Cloud service offering comprehensive ongoing user awareness training

WHAT WE DID WRONG

1. Underestimated the hackers

- Hackers are extremely sophisticated
- Malware is available as ‘open source’
- Free to all hackers
- Emotet used as carrier for other malware

WHAT WE DID WRONG

2. Firewall/network vulnerabilities

- Windows firewalls not ‘ON’
- Firewall logs not being saved beyond 24 hours
- No available firewall logs for the exact time when Emotet hit

WHAT WE DID WRONG

3. Inadequate cyber security awareness training

- Provided basic training on what to look for in suspicious email
- Training not comprehensive

WHAT WE DID RIGHT

1. Reliable, enterprise backup system

- Check backups daily
- Correct issues promptly
- Run test restores
- No data loss after Emotet

WHAT WE DID RIGHT

2. Isolated critical systems behind a firewall

- SCADA system
- Building access system
- Surveillance cameras

Conclusions

- Use an robust enterprise backup system
- Isolate critical systems behind a firewall
- Conduct user cyber security awareness training
- Employ expert, flexible IT staff
- Develop “Cyber Incident Response Plan”

Your Cyber Incident Response Plan

Print and post in a prominent location

1. IT Team response
   - Unplug user(s) from network (Limit scope of damage)
   - Get printed copies – Current IT contacts & system/administrator credentials
   - Determine what has happened (Identify Malware)
   - Call anti-virus & firewall providers

2. Contact experts for assistance
   - MS-ISAC - 866-787-4722, https://www.cisecurity.org/isac/report-an-incident
   - NCCIC (DHS) - 888-282-0870, https://ics-cert.us-cert.gov/Report-Incident
   - NJCCIC (NJ only) - 609-963-6900 x7865, https://www.cyber.nj.gov/report
   - WATER-ISAC (water/wastewater) - 866-426-4722, https://www.waterisac.org/report-incident

3. Business functions
   - Which business functions are up /down?
   - Identify critical business functions and how you will keep them running

4. Inform executives / elected officials
   - Identify scope of the damage
   - Time frame for each business function to be running again
   - List steps IT is taking to remediate the problem

Contact Information

Janice Zelnock, CGCIO

Supervisor of IT

The Brick Township Municipal Utilities Authority

1551 Highway 88 West, Brick, NJ 08724

voice: 732-701-4277

email: janice@brickmua.com