State of the Industry: Rural Cybersecurity

n-catt National Center for Applied Transit Technology

The National Center for Applied Transit Technology's (N-CATT) goal is to improve and make more efficient small-urban, rural and tribal transit service by educating staff about technology and other improvements.

An effective cybersecurity plan when implemented protects from attacks that compromise transit agency staff and riders, as well as their system and daily operations. This fact sheet reviews four elements:

1. The three types of cybersecurity hack most likely to occur
2. Types of preventative activities
3. Components of the plan
4. Funding options
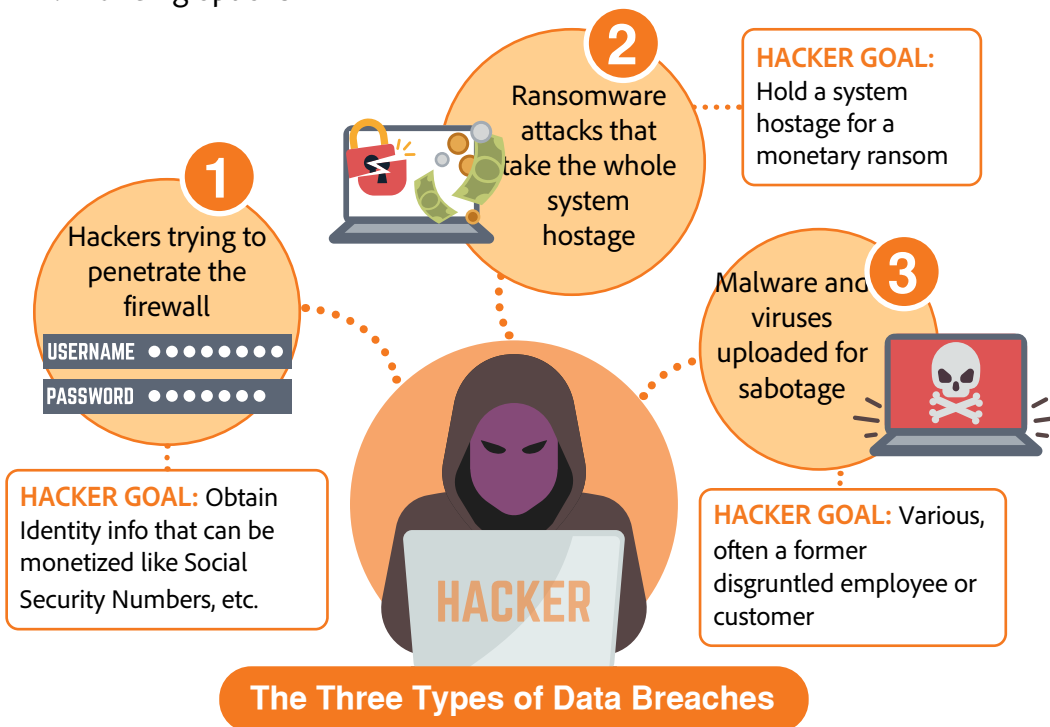
PREVENTATIVE ACTIVITIES

» Design a security system with a robust firewall. Include security measures like Two-Factor Authentication (2FA)

» Train Employees on Internet Security best-practices, do not assume knowledge

» Backup all organization data on a separate system

» Have an incident response plan

» Self assessment of its system before and yearly after the plan is implemented. (Use available tools, ex. download CATT tool on FTA)

1 Hackers trying to penetrate the firewall

USERNAME ● ● ● ● ● ● ● ●
PASSWORD ● ● ● ● ● ● ● ●

HACKER GOAL: Obtain Identity info that can be monetized like Social Security Numbers, etc.

2 Ransomware attacks that take the whole system hostage

HACKER GOAL: Hold a system hostage for a monetary ransom

3 Malware and viruses uploaded for sabotage

HACKER GOAL: Various, often a former disgruntled employee or customer

HACKER

The Three Types of Data Breaches

Prepare ➡ Detect ➡ Analyze ➡ Contain ➡ Eradicate ➡ Recover

COMPONENTS OF AN INCIDENT RESPONSE PLAN

Response Team
- » Management
- » IT
- » Legal
- » Safety/Security
- » External vendors (as relevant)

Roles
- » Point of Contact/Response Coordinator
- » Chief Information Officer

Procedure
1. Isolate the impacted systems
2. Investigate the breach & determine the method to mitigate
3. Activate or inform other departments like federal authorities, management, external communications, legal, etc.
4. Track the resolute, document what occurred and when
5. Once resolved, establish lessons learned using a post-incident report

TIPS

- » Speed is key. The faster the plan implements, the less likelihood for a breach
- » Account for remote staff, this can impact communications
- » Test the plan regularly and update accordingly
- » The Point of Contact should be someone with capacity for a new function
- » Communicating incidents to other agencies helps others avoid pitfalls

ADDITIONAL RESOURCES

- » TSA Surface Transportation Toolkit
- » American Public Transportation Association Securing Control and Communications Systems in Transit Environments
- » Cybersecurity & infrastructure Security Agency Awareness Program Law Enforcement Resources
- » Cybersecurity & infrastructure Security Agency Ransomware Guide
- » National Institute of Standards and Technology Security and Privacy Controls for Information Systems and Organizations.
- » Go to Federal Transit Authority website to see information about eligible expenses under the Formula Grants for Rural Areas Program