CENTER FOR DEMOCRACY & TECHNOLOGY

RANSOMWARE IN EDUCATION

BEST PRACTICES FOR PREVENTION & MITIGATION

January 2022

Schools Are a Prime Target for Ransomware Attacks

Cybercriminals are increasingly targeting schools with ransomware attacks — attacks that lock legitimate users out of their systems via encryption, while holding the decryption key for ransom. The impact of disrupted operations and lost instructional time, especially during remote learning, gives attackers significant leverage over schools.

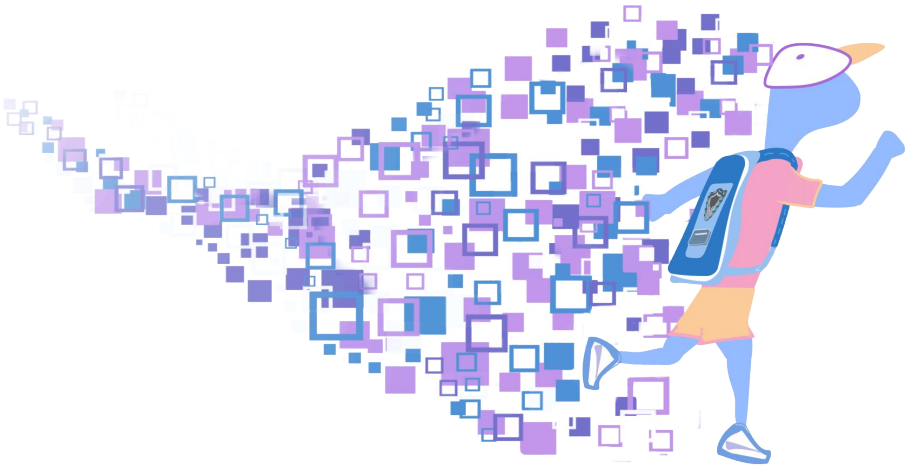
[FBI alerts of rise in PYSA ransomware targeting schools - SecurityMagazine.com]
[The 'real consequences' of ransomware against schools - StateScoop.com]
[Schools Brace for More Cyberattacks After Record in 2020 - Bloomberg.com]

The Impact of Ransomware on Schools

Ransomware attacks can cause significant damage to schools and their communities:

- Rob students of critical instructional time, especially during remote learning where teachers have limited options to continue instruction offline.
- Disrupt other school operations that rely on computer systems, such as managing enrollments, communicating with the community, or handling accounts and payroll.
- Include other cyber attack concerns, such as a data breach.
- Pull valuable resources from other areas of school operations to assist with response and recovery costs.

BEST PRACTICES: PREVENTION & PREPARATION



Prevention and Preparation Best Practices

There are steps schools can take to reduce the likelihood of a ransomware attack, or mitigate the severity if they are targeted, such as:

- Adhere to standard cybersecurity best practices.
- Keep data and systems backed up.
- Prepare alternative communication channels.

Cybersecurity Best Practices

Ransomware, like all malware, relies on vulnerabilities in systems to take root, meaning that standard cybersecurity practices are an important part of prevention. The following actions can help protect systems:

- **Keep system software up to date** to ensure that they have the latest security patches, making them vulnerable to fewer attacks.
- **Train staff on cybersecurity** so they do not inadvertently undermine system security.
- **Implement or encourage the use of security features** such as multifactor authentication or password managers.

Backing Up Data and Systems

One of the most important components of preparing for ransomware is backing up systems and data. Robust backups will significantly reduce the impact of an attack, as it strips the attackers of a primary source of leverage – access to data and systems.

There are practices that schools should consider to ensure their backups are maximally effective:

- **Maintaining off-site backups.** Backups that are not stored in the same place as the main system, ideally isolating them from certain forms of attack or incidents.
  - Air-gapped backups are completely disconnected from the main system, keeping them safe from a ransomware attack.
- **Use of WORM (write once, read many) backups.** These can be expensive (since the hardware cannot be reused), but if the original backup is sound, it cannot be corrupted by a later attack.

Alternative Communication Channels

Ransomware attacks can impact systems like email or office phones, which can disrupt communications at a critical moment. To ensure that staff can still communicate internally and externally in the event of an attack:

- **Establish alternative communication channels**, whether that is a phone tree using cell phones unconnected to school systems or alternative email accounts.
- **Test these communication channels regularly** to ensure that schools can reach everyone they need to reach in the event of an attack.

BEST PRACTICES: MITIGATION & RESPONSE

Restoring From Backups

However a school backs up its data, it is important to have a plan in place to restore from those backups. The following approaches can help smooth the process of restoring school systems:

- **Establish a response plan for restoration**, including determining which elements of the system need to be restored first, and who is responsible for each step.
  - Practice this protocol regularly to ensure any issues are worked out ahead of time, particularly as systems are updated.
- **Have a plan to test backups before restoring from them** to ensure that they are free from the ransomware virus. If the backup is not clean, using it to restore can further damage the system.

Communication During an Attack

Another important component of responding to a ransomware attack is communication, both internally with staff and externally with the community. The following considerations can ease that communication:

- **Establish communication plans ahead of time** to ensure that all affected parties are looped in as necessary.
  - For external communication, ensure it is accessible to all families who need it (whether that means translating the communication into various languages or levels of digital literacy, or ensuring it is available in a variety of formats).
- **Identify organizations that may be helpful partners** and need to be alerted after a ransomware attack (such as law enforcement or Information Sharing and Analysis Centers (ISACs)) and establish relationships ahead of time so they can be engaged in a timely manner.
- **Ensure communications are timely but accurate**, particularly for an evolving situation.

RANSOMWARE RESOURCES

Ransomware Resources

- **CDT's Guide on Ransomware in Education:** https://cdt.org/insights/ransomware-in-schools-best-practices-for-prevention-and-mitigation/
- **CDT's Cybersecurity in Education Training:** https://cdt.org/insights/training-module-cybersecurity-in-education-101/
- **PTAC's Data Breach Scenario Trainings:** https://studentprivacy.ed.gov/resources/data-breach-scenario-trainings
- **FTC's Guide on Protecting Children from Identity Theft:** https://www.consumer.ftc.gov/articles/0040-child-identity-theft
- **IBM's Guide to Ransomware Readiness, Response, and Remediation:** https://www.ibm.com/downloads/cas/EV6NAQR4
- **CISA's Guidance on Stopping Ransomware:** https://www.cisa.gov/stopransomware
- **Official Website for the Multi-State Information Sharing and Analysis Centers (MS-ISAC):** https://www.cisecurity.org/ms-isac/
- **Alantec Explainer on Different Approaches to Backing Up Data:** https://www.atlantech.net/blog/full-backup-vs.-incremental-backup-vs.-differential-backup-which-is-best

CDT'S VISION

PUTTING DEMOCRACY AND INDIVIDUAL RIGHTS AT THE CENTER OF THE DIGITAL REVOLUTION

CDT's Equity in Civic Technology Project

- *Provide **balanced advocacy** that promotes the responsible use of data and technology while protecting the privacy and civil rights of individuals.*
- *Create **solutions-oriented policy resources** that are grounded in the problems that currently confront policymakers, practitioners, and technology providers who work with them.*
- *Offer **technical guidance** that can be adapted and implemented by policymakers, practitioners, and the technology providers who support them.*

Contact Us

Equity in Civic Technology Project
Center for Democracy & Technology
CivicTech@cdt.org