The Three Most Essential Layers of Security Against Ransomware Attacks

Nationwide, ransomware attacks continue to grow more sophisticated and more devastating. While all industries are in the crosshairs, the risks are particularly acute for K-12 institutions. According to the FBI, 57% of America's reported cyberattacks targeted schools.

When successful, these attacks don't just shut down schools and cost districts hundreds of thousands of dollars: they also compromise students' critical personally identifiable information (PII). According to a recent study, the average ransom a district pays exceeds $125,000.

With so much on the line, it is essential that organizations take preventative action against ransomware attacks. A multi-layered defense strategy enables leaders to keep their data and communities secure.

Here are some foundational steps you need to take to ensure you can continue educating your community without interruption.

1 Take Control Over Your Network

Every day, hackers probe networks to take advantage of open ports and other vulnerabilities. The threat vector may start from a phishing scam, an insecure application, an HVAC system—anything that connects to the network. Once inside, the bad actors will encrypt your files and threaten to sell your critical data if their ransom is not paid.

With these threats looming, you must shore up your defenses before hackers strike. One of the best ways to do so is by achieving total visibility into your network. ENA's NetShield UTM is designed to do just that, giving you visibility and control of the traffic on your network. Offering user-level reporting and the ability to manage applications, ports, protocols, and more, ENA NetShield UTM constantly scans your network and critical systems to defend your community against an evolving array of threats.

This level of control and visibility makes it much harder for attackers to find a vulnerability in your network. However, no system is one hundred percent effective, which is why you also need to…

2 Backup Your Data, More Than Once

No matter the quality of your security system, vulnerabilities will remain. That's why you need to invest in high quality, multi-layered backup systems that, in case of an incident, will allow you to restore your essential data without disruption.

Your strategy should include local, cloud, and cold storage. Best practice is to follow the 3-2-1 rule – keep at least three copies of your data, store two backup copies on different devices or storage media, and keep at least one copy of your data offsite.

An effective storage platform will empower you to determine what data you want to back up and how often, while also encrypting your data in a secure, off-site location. To ensure your backup systems remain effective, practice restoring your systems and data by running tests when stakes are low to guarantee you'll be ready when disaster strikes.

ENA TrustBackup offers secure, encrypted, and customizable cloud backups backed by 24x7x365 customer support. And if you already have a cloud backup utility, make sure your off-site backup storage solution meets your organization's needs. A secure and effective home for your data—such as ENA TrustVault—will ensure data redundancy and resiliency, limit access to only those who need it, and scale easily to meet evolving needs. That way, no matter when disaster strikes, you can rest assured operations will continue uninterrupted.

And if your organization already has a layered backup strategy, you should also be sure to…

3 Train Your Users. Then Train Them Again

No matter how many layers of security you put in place, one stray click can let ransomware into your network. In fact, last year saw an 18% increase in the number of publicly disclosed incidents—a continuation of the previous year's trend. This rate of attack comes out to more than two incidents per school day throughout 2020.

One of the best ways to mitigate user-induced breaches is through regular best practices training with your network users. Establishing an annual cadence of phishing testing and feedback is a great place to start. Sharing results of a testing period is a risk-free way to educate your user community about the strategies threat actors are successfully using elsewhere. Further, promoting widespread threat awareness will serve as an additional and effective line of defense against ransomware attacks.

To discover how ENA's robust suite of security solutions can strengthen your organization's defenses against ransomware attacks, visit www.ena.com/security.

About ENA by Zayo

ENA delivers transformative connectivity, communication, cloud, cybersecurity, and technology services. Our 99% customer satisfaction rating and world-class net promoter score (NPS) demonstrate our commitment to delivering exceptional customer care. For more information, please visit **www.ena.com**, call **866-615-1101**, or email **info@ena.com**.

ena® by zayo

082215