M247

COHESITY
ASSOCIATE PARTNER
SERVICE PROVIDER

Ransomware tip sheet for further education institutions

5 ways ransomware attacks backup... and how you can prevent it

How universities can prevent, detect and rapidly respond to ransomware attacks on backups

The National Cyber Security Council (NCSC) has recorded a significant increase in the ransomware attacks affecting further education establishments in the UK over the last 12 months. As a result, the latest NCSC guidelines include advice on how to prevent malware and ransomware attacks.

The first step in this journey is to better understand where data is stored and how you can protect it.

This tip sheet describes 5 ways university IT staff can overcome the risks of data loss when ransomware attacks are targeting data backup.

The impact of ransomware on backup data

Backup and recovery solutions are designed to protect your organization, but sophisticated malware like Locky and Crypto are now targeting your backup data. Not surprising, considering the rise in frequency and breadth of ransomware attacks. The first ransomware payment—circa 1989—set the stage for hackers everywhere to begin locking up the data of unsuspecting targets and holding it until owners paid to get it back. Now analysts predict a ransomware attack on businesses will happen every 14 seconds—at a cost of billions to global organisations. That's why it's important to keep these five considerations in mind when you're strategizing how best to prevent, detect, and rapidly respond to a ransomware attack on your backups:

1. Sophisticated ransomware attacks make your insurance policy—your backups—a liability

Cyber criminals are now aggressively targeting shadow copies backup data—to gain full control, or worse, destroy what has long-been considered your insurance policy to business continuity. Their more sophisticated attacks enter a primary environment from an endpoint and head straight for your backups—where 80 percent of enterprise data is now stored—deleting or compromising everything there before taking over the production environment. What's needed to prevent ransomware attacking your backup is a multi-layered defense. Original backup jobs should be kept in an immutable state, and never made accessible to prevent being mounted by an external system. Also, multi-factor authentication (MFA) and write once read many (WORM) capabilities for the snapshot are must-have features.

Ransomware by the Numbers

- Every 14 seconds, ransomware attacks
- 700% growth since 2016
- 35% of attackers get paid
- $2B in financial losses
- $11B in financial, productivity, and downtime losses!

"Ransomware writers are aware that backups are an effective defense and are modifying their malware to track down and eliminate the backups."

—CSO MAGAZINE

Contact our experienced team today to find out more

sales@m247.com 0808 301 9688 m247.com

5 ways ransomware attacks backup...and how you can prevent it

2. Expanding attack surfaces expose backups to ransomware attacks

Exploding data growth (IDC estimates 175+ zettabytes of data will exist by 2025) and mass data fragmentation—the growing proliferation of backup data across different sprawling silos—have combined to widen your organization's attack surface. As a result, your backup data has become more accessible to cybercriminals. Preventing ransomware from succeeding in the first place starts with reducing your enterprise attack surface and knowing what data you have and where it is located. A unified solution for connecting infrastructure, workloads, and backup locations arms your organization against ransomware by eliminating mass data fragmentation.

3. Attacks on backups made easier by intermittent monitoring

Cyber threats don't always originate from outside of an organization; they can be launched internally, too. Imagine a disgruntled employee trying to modify or delete a large set of data. Relying exclusively on backup data-ingest change rates to detect such behaviors is insufficient, hence your organization must be able to detect an attack in real time.

What's needed is a solution that can continuously monitor and detect smaller change rates by analyzing files and audit logs – even when you're not paying close attention. The right backup solution will protect your organization from cyber attacks every second of every day.

4. Public cloud providing entry point for ransomware's criminals

The cloud is quickly becoming a point of entry for cyber attacks, which is putting your backup data at risk. In fact, McAfee estimates one in four public cloud users today have experienced data theft! The bottom line is this: Data in the cloud is not immune to ransomware. The public cloud may be cost-effective for backups, but it also means decreased data visibility. Staying ahead of ransomware requires a backup and recovery solution that offers a single dashboard.

Being able to see, manage, and take action fast on your backup data – whether residing on-premises or across public clouds – will help your organization protect itself from ransomware attacks.

5. Long backup and recovery cycles adding to your ransomware pain

If your enterprise relies on legacy backup that require synthetic fulls and falls victim to a ransomware attack, your IT team can spend days (even weeks!) in recovery mode. A recent Ponemon Institute report puts the average cost of a single ransomware attack at $5 million due primarily to productivity loss, systems downtime, and theft of information. What's needed is a backup and recovery solution that responds fast to ransomware attacks and lets you quickly locate and delete infected files across your global data footprint – including the public clouds. Also needed is instant mass restore capabilities, which enable recovery of hundreds of virtual machines instantly, at scale, and to any point in time.

Enabling further education institutions to mitigate against ransomware threats

Educational establishments want reassurance that their data is safe, that they meet all NCSC security guidelines and that IT staff are on top of data compliance requirements and are able to respond to quickly respond to threats.

We help institutions like yours evaluate risk, mitigate against threats and develop a robust data management strategy. Helping you ensure all the gaps are closed and that attackers can't exploit your data or infrastructure. Our backup as a service solution (BUaaS) platform is an orchestration of data consolidation, protection and security, empowering you and your staff to stay focused on what matters the most.

Contact our experienced team today to find out more

sales@m247.com 0808 301 9688 m247.com