THE MOST OVERLOOKED SECURITY ISSUES FACING THE FINANCIAL SERVICES SECTOR

Data is a major part of the role of any CISO. When it comes to the financial services industry, data is even more important and valuable than in other industries. Securing storage and backup systems isn't always obvious and isn't always the focus of many CISOs or their teams. I admit that it wasn't part of my focus until quite recently.

So, what is the big picture of securing storage and backup? Is this a Cinderella area in the pursuit of business security? How can you prepare? And where do you go from here? I will share with you my views in this article.

All Eyes On Storage And Backup

It's no secret that modern security is focused on data, particularly in the financial services industry. The rise – and sophistication – of ransomware attacks has been documented by all parties concerned.

From industry publications like Bleeping Computer...

"The ALPHV ransomware operation exploits veritas backup exec bugs for initial access. U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds these 3 security issues to its list."

...to analysts like Gartner...

"Harden the components of enterprise backup and recovery infrastructure against attacks by routinely examining backup application, storage and network access and comparing this against expected or baseline activity."

...to governments finally addressing the issue, like in last year's White House memo:

"Test the security of your systems and your ability to defend against a sophisticated attack."

Ransomware is focused on data. As such, the key to mitigating (and ideally neutralizing) that threat is to secure data in storage and backup.

We tend to think of backups as the final layer of protection against ransomware, though in reality they are simply another repository of data in storage, ready to be harvested if not appropriately secured.

This begs the question: are we as Chief Information Security Officers (CISOs) and other security leaders currently focused on the most pressing risks?

The Unspoken Gap

The value of business data is growing annually in virtually every organization. Malicious actors recognize this fact, so data-centered attacks continue to grow both in number and sophistication.

Are we really rising to this challenge as CISOs and security leaders? Have we spent enough time analyzing and reinforcing those darker parts of our storage and backup infrastructure that any smart threat would target? This industry-wide oversight is exactly why so many of these attacks succeed.

There are other myths that many CISOs and security leaders believe which feed the current exponential growth of attacks and further demonstrate the industry's continued failure to harden storage and backup systems. They are the greatest current oversight in cybersecurity.

The Shift In Voice And Focus Of The Financial Services CISO

The truth? In a cloud-fuelled world, storage layers deserve as much attention as computing and networking layers. Cloud providers offer cloud storage as a separate service, carrying a separate set of risks – access keys in AWS S3 storage, for example.

Storage security issues aren't limited to the cloud either; they spread across the full spectrum of hybrid and on-premise infrastructures. All these modes of storage constitute separate systems, but for whatever reason they haven't enjoyed the same attention from infrastructure and security experts as those on other layers.

The need for change is also reflected in this Financial Services Research Report, which analyzed the state of storage & backup security:

- Two-thirds believe that a storage attack will have 'significant' or 'catastrophic' impacts.
- 60% are not confident in their ability to recover from a ransomware attack.
- Two-thirds say that securing backups and storage was addressed in recent external audits.

Back to the Table of Contents

Heading For A Better Future... But How? Four Steps For Success

Now that we understand the problem, what's the solution?

Many CISOs already follow the steps below when faced with a new threat. While I'm not here to deliver a tutorial that teaches a fisherman how to fish, I note that it is critical to revisit the fundamentals: in this way, we will ensure that we're covering the increasing storage & backup security problem in the correct and thorough way that it deserves. At this point we're playing a game of catch-up, and can ill-afford missteps.

Use the following four steps to form the foundation of our storage and backup security approach:

1. Education

The first step is to understand the capabilities of our storage and backup devices. In our real environment, what do we have (not just in theory)? Specifically, which vendors do we use, how are their technologies deployed, and how are roles and responsibilities defined?

An excellent place to begin in this phase is to perform an initial assessment of our storage and backup security. This assessment will detail any risks identified and include the corrective steps for remediation.

The NIST Special Publication 800-209; Security Guidelines for Storage Infrastructure (co-authored by Continuity) is an excellent resource for those looking to develop their storage infrastructure knowledge. It provides a thorough overview of current storage technologies and their relative risk landscapes.

2. Definition

Once we get the lay of the land, we should define 'secure enough' baselines of our storage and backup environments. The map of the baselines needs to be detailed since these environments are complex and the attack surface is convoluted.

For instance: what kind of roles are needed? What kind of controls do we want to have? What level of auditing do we expect?

Once we define these baselines, it's much easier for the storage admins to ensure that they're fully implemented, audited and monitored

We also need to define threats and robust security protocols.

3. Implementation

With knowledge accrued and threats defined, the rubber needs to meet the road. Now comes the stage of implementing the controls that were previously defined. Please note: usually when the initial gap analysis is done (remember step 1), we will likely end up with a long list of deviations. Now's the time to straighten them out.

Implementing automation in performing these changes is key.

Another practice I recommend here is to build KPIs and automatic measurements for the predefined baselines, in order to make sure they are always met.

So, in essence, at this stage security leaders must:

- Harden storage
- Implement controls

4. Ongoing risk management

Storage and backup security demands active, ongoing risk management. As threats continue to evolve, so must we. In order to keep up, we can lean on:

- Measurement
- Reporting
- Automation

While the above steps might seem obvious, until now their implementation within the area of storage and backup has been less so. CISOs need to be in dialogue with the IT infrastructure teams to ensure that this set of risks is being taken as seriously as it needs to be.

Conclusion

Data is the bread and butter of the 21st century. And just as these valuable resources have always been securely stored and protected, so must an organization make significant investments in data protection, and storage and backup hardening. CISOs have the skill to do it; many simply lack the know-how. The problem needs to be reframed in the minds of security experts, and fast, as the problem of ransomware is already surging.

CONTINUITY

Back to the Table of Contents