The Ins And Outs Of File-Centric Security

Devolutions

THIS ARTICLE WRITTEN BY MATTHEW DAVIS, TECHNICAL WRITER, IS PART OF OUR GUEST BLOG SERIES.

PLEASE CONTACT US IF YOU WOULD LIKE TO BE FEATURED ON OUR BLOG.

In today's enterprise, securing your organization's perimeter isn't enough. You need to think beyond your business's walls by considering how remote workers, partners, and suppliers are accessing your systems and data. This involves ensuring sensitive files are always under your control. Here's where to start in that regard.

Presumably, your organization has some pretty strong internal defenses in place. Access controls, network monitoring, firewalls, antimalware tools, endpoint management software...you get the idea. In 2019, that sort of thing is basic cybersecurity.

You need to secure your systems. You need to control the mobile devices used by staff. You need to guard yourself against intrusion attempts. You know this.

But do you also know that you need to take measures to protect your data?

I don't just mean managing access within your business's perimeter. We live in a culture of collaboration. An era in which sensitive documents are shared across devices and organizations with greater frequency than ever before.

In such an era, the basics are no longer enough. You need to take things a step further to ensure you maintain control over your most critical assets no matter who they're shared with.

You need a file-centric security solution.

Such a solution should meet a few key criteria. First and foremost, it needs to be easy to use for both end users and IT staff. Secondly, it should offer extensive monitoring and logging functionality. Lastly, it should allow your IT department an extensive, intricate level of control over your data.

There are a few reasons for this, which I'll discuss in detail below.

Visibility Is Your Most Powerful Weapon Against Attackers

In 2015, we bore witness to the largest data breach in history, dubbed the Panama Papers. Law firm Mossack Fonseca saw over 2.6 terabytes of highly-confidential information exfiltrated by anonymous hackers, who then released the data through the Consortium of Investigative Journalists. Since then, the law firm has closed its doors and we've seen multiple charges of tax evasion and money laundering leveled against its former clients.

Digging a bit deeper reveals how the Panama Papers incident was caused by multiple egregious security blunders.

"The story [of the Panama Papers] is actually about a company with third-rate security that got exploited by a routine hack," wrote eWeek's Wayne Rash in 2015. "What's clearly lacking is even the most basic attempt at protecting the firm's client data... Apparently, none of it was segmented, none seemed to have restricted access to specific people, none of it was encrypted, and nobody was paying attention to network traffic."

The lesson here is pretty obvious. Had the firm been paying even a modicum of attention to its data, it could have prevented the bulk of what happened. See, like any criminal, hackers prefer to operate in secret – their worst enemy is an organization that's aware of its assets.

With that in mind, whatever file security software you install should allow you to see where each and every asset is at any given time. You should be able to determine, at a moment's notice, who has access to a file, what they've done with that access, and on what devices that file is stored.

More importantly, you should be able to exert total control over those files. Let's say, for instance, someone has shared a product blueprint with a manufacturer. You'll want to ensure that blueprint cannot be modified or shared outside the vendor's walls.

Depending on your industry, you might even be required to maintain organized access logs for your data – **regardless of how it's been shared**.

If Your File Sharing Solutions Aren't Convenient, They're Useless

I've heard it said that cybersecurity is an eternal war between security and convenience – and convenience is winning. We are in the midst of a technological renaissance, and the days when an organization's IT department could exercise complete control are well behind us. When implementing any product or solution, you **need** to consider how it impacts the end user.

If you don't, employees will simply circumvent whatever security measures you've put in place. You **cannot** stop them from doing so – not without fostering resentment and hostility. What you need to do instead is strike a balance.

Work with them to find a file sharing platform that fits their needs and meshes with their workflow. Examine the tools they're already using in the workplace, and find something that works in a similar fashion. Work from the understanding that everyone needs to be involved in cybersecurity, and you'll be all the better for it.

Never Assume You Aren't A Target

Extensive file controls. Access monitoring and logging. Streamlined collaboration for end users. These features are the cornerstones of an effective file security platform.

At this point, maybe you're operating on the belief that your business is too small to catch the attention of hackers. Maybe you think that because you're not a major law firm or a multinational corporation, you're not in anyone's crosshairs. Let me dispel you of that notion right now.

Hackers are increasingly targeting small and mid-sized businesses. They know that larger organizations are likely to have extensive security measures in place and a well-funded team of IT professionals to enact them. In addition to tending towards the shadows, hackers will usually seek the path of least resistance – they'll usually go for the easiest targets.

And there's no easier target than a poorly-secured small business that believes it's safe from attack. No matter the size of your organization, the advice I've offered in this piece holds true. Cybersecurity is **never** something you can afford to ignore.

That's true whether you're a small, family-owned business or a globe-spanning enterprise.