SIMPLY SHAREPOINT

Your Guide to SharePoint and the Modern Microsoft 365 Toolkit

SHAREPOINT

SharePoint Hack 2025: What It Means For On-Prem vs Online Security

I've been chatting with some folks in the cybersecurity space lately and a topic came up that I just had to share with you. You might have seen the stories in the news about a rather significant SharePoint hack that hit government systems across Europe and the US recently. It's a big deal, and it brings to light a crucial distinction I often talk about: the difference between SharePoint on-premises (sometimes called 'on-prem') and SharePoint Online.

Now, I know what some of you might be thinking: "Hack? SharePoint? Is my data safe?" And that's a fair question! But before you panic, let's unpack this a bit, because it's not quite as straightforward as it might seem on the surface.

The Latest SharePoint Stir: What Happened?

The hack that's been making headlines involves **on-premises SharePoint servers**. What does that mean exactly? Well, for a lot of larger organisations, especially government agencies, they have their SharePoint servers physically sitting in their own data centres, managed by their own IT teams. Think of it like owning your own house and being responsible for all the maintenance and security.

For companies that choose to go 'on-prem' it allows them to have greater control over their data – critical in an era where more organisations care about 'data sovereignty' and compliance regarding data management laws. It also allows greater flexibility in terms of adapting and integrating them into their systems, which is important when organisations need to scale quickly. Many companies have migrated away from the cloud, but it's come with a greater responsibility for companies to manage their security more effectively.

This particular breach exploited what's known as a "zero-day" vulnerability introduced in a Microsoft security update across on-prem systems. In plain English, that's a flaw in the software that even Microsoft didn't know about yet, or at least hadn't released a fix for. Attackers found a way to run their own code on these unpatched servers, gaining access to sensitive data. It's like finding a hidden, unlocked window in someone's house that even they didn't know was there.

The impact has been considerable, affecting government entities, energy companies, and universities. Hackers were able to access critical servers and shutdown access, as well as potentially stealing security information. It's as yet unclear what the objective of the hackers were, but it will mean that organisations across the globe will have to spend millions updating security protocols, validating information, and checking for potential backdoors hackers might exploit to maintain persistence. It's a stark reminder of the damage that can be done, even at large institutions with significant resources, by sophisticated hackers.

SharePoint Online: A Different Ballgame

Here's the really important bit I want to highlight: **SharePoint Online, which is part of Microsoft 365, was NOT impacted by this particular vulnerability.**

Why is that? Because with SharePoint Online, Microsoft takes on the heavy lifting of security, maintenance, and patching. It's like living in a serviced apartment complex where the building management looks after all the security, repairs, and updates. They have dedicated teams whose sole job is to monitor for threats, apply patches instantly, and ensure the infrastructure is robust.

This is a fundamental difference. When you're using SharePoint Online, you're benefiting from Microsoft's enormous investment in cybersecurity. They have global teams working 24/7 to identify and mitigate threats, often before they even become public knowledge. This includes things like:

- **Automatic Updates and Patching:** You don't have to worry about manually applying security updates. Microsoft handles it all in the background, ensuring your environment is always running the latest, most secure version.
- **Robust Infrastructure:** Microsoft's data centres are built with multiple layers of physical and digital security, designed to withstand sophisticated attacks.

- **Advanced Threat Protection:** They employ a suite of tools and technologies to detect and prevent malware, phishing, and other cyber threats.

That being said, it's important to note that relying on Microsoft's security is not a perfect solution either. Sadly, you don't have to look too far for massive security breaches on Microsoft's part – just two months ago nearly 184 million Microsoft and Google logins were leaked after they were found on an unsecured database.

"More Effective Architecture and Security Measures Could Have Prevented This"

I had a chat with Adam Maurer, the COO of Connecting Software, a company that works with secure integrations for high-security sectors. He made a really interesting point about this breach. He said, "This day-one exploit of Microsoft's systems resulted from a massive and overlooked vulnerability that allowed attackers to execute arbitrary code remotely on unpatched on-premises SharePoint servers across several key sectors. It exploited a deserialisation flaw within Microsoft's code, enabling attackers to gain control and access sensitive data."

"Rather than a call to move away from on-prem, these attacks highlight to businesses the importance of a hardened security posture with zero-trust configuration, Data Loss Prevention (DLP) software, proper firewall settings including intrusion detection and devices like data diodes as a key additional element for securing air-gapped networks."

Now, these terms might sound a bit technical, but let me break it down simply.

- **'Zero-trust',** a key concept in cybersecurity means that in either side of an interaction, both sides must be able to independently verify the information and credentials of the people (or programs) involved and that no critical information should change hands until that happens.

- **Data Loss Prevention (DLP) software** are programs that classify critical data and block it from being transmitted improperly. These programs can prevent users from using the 'copy' function on important files and prevent them from being moved elsewhere through different methods.

- **Firewalls and intrusion detection**– installed on almost every computer and most importantly, at the entry to a network, with varying degrees of sophistication, are programs designed to identify and flag potentially damaging actions and code and stop them. When combined with intrusion detection, which is able to detect and alert systems to potential intruders they can be an effective way of preventing attack

- **Air-gapped networks** are essentially networks that are completely isolated from the internet and any other external networks. Think of it as a computer that's never, ever been connected to Wi-Fi or a network cable. It's the ultimate in isolation. For highly sensitive government data, this level of separation provides an incredibly strong barrier against external attacks. If these critical networks were cut off from the internet, or only accessible through a secure Virtual Private Network (VPN), a breach would have been prevented regardless of the vulnerability that was introduced.

- **Data diodes** are hardware devices that enforce one-way communication. Imagine a pipe where water can only flow in one direction. Data can go *out* from a super-secure network, but nothing can come *in*. This is crucial for stopping data from being stolen (exfiltrated) while still allowing necessary information, like monitoring data, to be shared. It's important to note that exposing your resources like SharePoint to the internet will always run risks, but data diodes can help minimise this.

Adam's added that "While none of these measures are perfect on their own, they would have prevented these hackers from moving around sensitive networks unimpeded, vastly improving organisations' ability to safeguard important systems."

He argued that this should serve as a "wake up call" to companies and agencies all around the world that, in the age of AI and quantum computing, it takes mere seconds to exploit vulnerabilities, so a multi-layered approach to securing your environment is vital.

My Take: Working Smarter, Not Harder, with Security in Mind

So, what's my angle on all of this? It's about **making informed choices about your SharePoint strategy to work smarter, not harder, when it comes to security.**

For organisations that don't have the resources or expertise to build their own networks, staying on the cloud will continue to make sense. But as many organisations move to on-prem SharePoint, this hack illustrates that the added benefits of control over data come with the responsibility of being more vigilant than ever about outside cybersecurity threats.

This recent breach serves as a powerful reminder:

- **On-premises means on you.** If you choose to host SharePoint yourself, you are taking on the full burden of security, maintenance, and patching. This requires a significant ongoing investment in expert staff, robust processes, and advanced hardware solutions. Companies that want to go on-prem must be willing to make these improvements.
- **Security is more important than ever.** Hackers grow in sophistication every year, and even when using cloud Sharepoint, you still have a vital role to play. This includes things like:
- **Strong Passwords and Multi-Factor Authentication (MFA):** This is your first line of defence.
- **Careful Permissions Management:** Ensure only the right people have access to the right information.
- **User Training:** Educate your team on cybersecurity best practices, like recognising phishing attempts. This is a key element for companies looking to be more secure, regardless of whether they are online or on-prem.
- **Data Loss Prevention (DLP) Policies:** Set up rules to prevent sensitive information from leaving your organisation.
- **Cybersecurity insurance:** can help companies reduces their exposure to additional costs coming from cyberattacks

My 20+ years in this space have shown me that for many workplaces, relying on cloud versus on-prem SharePoint is a difficult decision that depends on your business's broader context. For some, moving to SharePoint Online in Microsoft 365 streamlines operations, enhances collaboration, and can free up your internal IT team to focus on strategic initiatives rather than constantly battling the latest zero-day exploits on your own servers. For others, moving to on-prem allows more peace of mind in regard to sensitive data and compliance, and can, in many cases, be *more* secure if you are willing to make the investment in proper security.

Your Next Step

If you're currently using SharePoint on-premises, this news should prompt a serious conversation within your organisation about your security posture and whether your current setup truly provides the level of protection you need.

And if you're already on SharePoint Online, take a moment to appreciate the peace of mind that comes with knowing a dedicated team of experts is constantly working to secure your data. But also, use this as a prompt to double-check your own internal security practices – things like strong passwords, MFA, and sensible sharing policies are still absolutely vital.

Ultimately, my goal is to help you use SharePoint to work smarter, not harder. When it comes to securing your business, there are plenty of difficult decisions to make – but ultimately, an investment of time and money in cybersecurity is necessary.

Stay safe out there, and happy SharePointing!

SHARE:

PREVIOUS POST
5-DAY SHAREPOINT CLEANUP GUIDE: FIX YOUR MESSY DOCUMENT LIBRARY FAST

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment *

Name *

Email *