Potomac Institute for Policy Studies presents

Tech Happens© *provides short articles on critical technology and policy issues, their effects on our lives today, and impact to the future.*

SharePoint Servers Hacked

July 25, 2025

The recent news about Microsoft SharePoint hack brings to light the major issues with today's implementation of cybersecurity and hardware security. In this case, a coding flaw gave rise to a vulnerability resulting in a security hole that could be used to gain control over an in-house SharePoint server. The flaw was most likely discovered by hackers because the US government discovered a related flaw, posted information about it without fully remedying the flaw, and then the Chinese-based "Salt Typhoon" group exploited similar vulnerabilities. AI-based software development is not likely to prevent such vulnerabilities because they are based on existing code that can contain flaws. Security systems might be able to examine code to identify vulnerabilities, but such technology has not yet fully "happened." The fundamental problem is that all computing, both hardware and software, regard program code as the same as data (which is fundamental to computers), but that such code can be altered and is not always thoroughly authenticated.

There is extant technology to authenticate every packet and every attempt to inject code into executable processes but is considered "a pain" because it consumes computing resources and limits access that would otherwise require onerous registration processes. Imagine if every device that wants to connect to the Internet required permission to do so! However, for applications requiring security for which the harm of a hack might be great, keeping hackers is possible by using secure hardware solutions that require any and all code execution commands to be "signed." Energy needs and complexity might increase, but the technology that combines algorithm advances with semiconductor state-of-the-art progress makes better security possible.