MOVEit: Testing the Limits of Supply Chain Security

Since late last month, a Russian cyber-extortion gang has been exploiting a flaw in a widely used software known as MOVEit. The program is used by many organizations to securely transfer data and share files. Meanwhile, hundreds of commercial businesses (e.g., BBC, Shell, British Airways, Boots, Zellis) and government agencies (e.g., U.S. Department of Energy, the Louisiana Office of Motor Vehicles, the Oregon Department of Transportation, the Minnesota Department of Education, the Novia Scotia government) confirmed being impacted by the attack. As Jen Easterly, director of the Cybersecurity and Infrastructure Security Agency (CISA) pointed out, unlike the stealthy SolarWinds hacking campaign, the MOVEit attack was relatively superficial and caught quickly. However, it highlights how vulnerable organizations remain to cyberattacks even after years of investments to improve security postures. This begs the question: are our existing cybersecurity practices really optimized for today's dynamic threat landscape?

The MOVEit zero-day attack seems to affirm the White House's National Cybersecurity Strategy's call to shift liability to organizations that fail to make reasonable precautions to secure their software. The strategy acknowledges the fact that "poor software security greatly increases systemic risk across the digital ecosystem and leaves American citizens bearing the ultimate cost." A special focus of the strategy is on software developed by unvetted third parties that is embedded into commonly used programs, potentially allowing hackers to exploit flaws. Whether the National Cybersecurity Strategy will have any impact that can help mitigate the exploitation

of software vulnerabilities such as MOVEit remains to be seen.

Remember that the Biden Administration's National Cybersecurity Strategy is not an executive order but a plan on how to shape a more consistent approach to cybersecurity at the national level. Execution of the strategy would require passage through Congress. Given the current deep political division, getting the necessary buy-in from both parties will be challenging. It is likely that the ambitious plans will initially be applied to critical industries that the government has authority over. This can be done by setting standards within these sectors and enforcing specific procurement requirements and security standards across applicable federal agencies. But even in those cases, it can take years for those rules to take effect.

Meanwhile, we have to acknowledge that spending your way to a secure state is costly, builds a false sense of security – and simply doesn't work. Instead of exclusively focusing resources on preventing an attack, it's important to develop a plan to mitigate the impact when a successful attack occurs. Forward-thinking organizations are adopting a new strategy to cope with today's increased cyber threats, called cyber resilience.

The need for cyber resilience arises from the growing realization that traditional security measures are no longer enough to protect systems, data, and the network from compromise. The objective of cyber resilience is to ensure that an adverse cyber event, whether intentional or unintentional, does not negatively impact the confidentiality, integrity, and availability of an organization's business operation.

A cyber resilience strategy is vital for business continuity and can provide a range of benefits prior, during, and after a cyberattack, such as:

- **Enhanced Security Posture:** Cyber resilience not only helps with responding to and surviving an attack. It can also help an organization develop strategies to improve IT governance, improve security across critical assets, expand data protection efforts, and minimize human error.
- **Reduced Financial Loss:** According to the IBM Cost of a Data Breach Report 2022, the average cost of a data breach is now $4.35 million globally. In addition to financial costs, the reputational impact of data breaches is increasing due to the introduction of general data protection laws and stringent data breach notification requirements. Cyber resilience can help minimize recovery costs by accelerating time-to-remediation.
- **Improved Compliance Posture:** Many industry standards, government regulations, and data privacy laws nowadays propagate cyber resilience.
- **Enhanced IT Productivity:** One of the understated benefits of cyber resilience is its ability to improve the daily IT operations, including threat response and ensuring day-to-day operations run smoothly.
- **Heightened Customer Trust:** Implementing a cyber resilience strategy helps improve trust as it enhances the chances of responding to and surviving a cyber-attack, minimizing the negative impact on an organization’s customer relationships.
- **Increased Competitive Edge:** Cyber resilience provides organizations a competitive advantage over companies without it.

As we wait for the National Cybersecurity Strategy to come to maturity, organizations must augment their current cybersecurity strategy with a focus on cyber resilience. Most

cyber resilience initiatives leverage or enhance a variety of cybersecurity measures. Both are most effective when applied in concert.

Advertisement. Scroll to continue reading.
https://www.securityweek.com/moveit-testing-the-limits-of-supply-chain-security/