Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Microsoft Server Hack Sparks Debate On Victim Expectations

By **Ben Kochman**

Law360 (March 12, 2021, 9:12 PM EST) -- Following a cyberattack on Microsoft's Exchange email servers by hacking crews that the software giant says target law firms and defense contractors, some cybersecurity pros are calling for companies to put in place safeguards that would apply even if their vendors are hacked.

The potential looting of victim companies' email files by threat actors whom Microsoft has linked to the Chinese government is yet another indication that any third-party vendor can be vulnerable to attack — even one of the world's biggest companies, cybersecurity experts say. A top White House official said Friday that the scope of these threat actors is still being probed.

Given how often vendors are breached, organizations should consider taking measures to protect their data or mitigate the damage of incidents, going beyond existing efforts to vet the security of third-party products, some cybersecurity pros say.

"We need to turn our attention to expecting that software is going to have issues, and planning for the failure," said Serge Jorgensen, co-founder and president of Sylint, a cybersecurity and data forensics company.

"We expect cars to get in wrecks, therefore we have seatbelts and air bags," Jorgensen said. "If we don't enact those sorts of protections and controls in the digital world, we will just continue as we have been."

News that hackers were exploiting flaws in Microsoft's Exchange servers came as both public and private organizations were reeling from two other breaches at third-party companies: file-transfer software giant Accellion Inc. and IT management software provider SolarWinds Corp.

The Accellion breach has affected entities as varied as the **law firm** Jones Day, New Zealand's central bank, Washington's state auditor, Australia's securities regulator, Harvard's business school, the rail carrier CSX Corp. and the **supermarket and pharmacy chain** Kroger. Meanwhile, the SolarWinds episode **led to breaches** at nine U.S. federal agencies — including the U.S. Department of Homeland Security — and potentially more than 100 private companies, U.S. authorities have said.

Given the breach-heavy climate — conditions that were **only inflamed** by a global pandemic that has made it easier for hackers to find a way into networks — it might be easy for potential targets to throw their hands up, particularly if the attackers are believed to be sophisticated, nation-state-backed spies.

But taking such an approach would only make it easier for hackers to make their way into victims' systems, said Michael Daniel, the former White House cybersecurity coordinator from 2012 to 2016 who now serves as president and CEO of The Cyber Threat Alliance.

"I'm worried about creating a fatalistic attitude among businesses that there's nothing that you can do about your cybersecurity," Daniel said in an interview. "A dedicated nation-state is a very difficult opponent, but that doesn't mean there's not value in making it hard on them. You can still do things to reduce the impact of incidents and be able to recover from them when they do happen."

Victims of data breaches that started with intrusions into third-party vendors are still likely to **face questions** from regulators, clients, investors or customers about whether they took steps to make employees verify their identifies through two-factor authentication or routed employee traffic through virtual private networks, or VPNs — which themselves **can be hacked**.

Organizations should also work to update their networks to run the latest software as quickly as possible, cybersecurity experts say.

Microsoft has released versions of its Exchange products that include fixes for the security vulnerabilities, though organizations that have not updated to the newest software have been hit by groups of hackers exploiting the Exchange flaws to launch ransomware, in which they demand payment to unlock frozen systems or retrieve stolen files.

Microsoft has said in blog posts over the past week that the hackers behind the original attack were likely Chinese state-sponsored, and that one of the groups, which it dubbed "Hafnium," has targeted a range of industries including law firms, infectious disease researchers, higher education institutions and defense contractors.

But White House national security adviser Jake Sullivan said in a briefing Friday that U.S. authorities are not yet prepared to attribute the attacks, and that the "scale and scope" of the intrusions are still under investigation.

The recent spree of third-party vendor breaches, and news that FireEye Inc., one of the world's largest cybersecurity companies, **suffered a cyberattack** — an intrusion that led to the discovery of the SolarWinds breach — should make people think twice about reflexively blaming a breach victim before a full investigation into the episode, said John Reed Stark, the president of data breach response and digital compliance firm John Reed Stark Consulting LLC.

"Data breaches are inevitable. If you have been the victim of a cyberattack, it doesn't necessarily follow that you've done something wrong," Stark said. "If Microsoft can get hacked, it pretty much proves that anyone can get hacked."

--Editing by Nicole Bleier and Kelly Duncan.
