CYBERSECURITY

Biden to issue executive order amid dual hacking emergencies

Christian Vasquez, E&E News reporter • Published: Monday, March 8, 2021

White House deputy national security adviser for cyber and emerging technology Anne Neuberger briefed reporters last month on the Biden administration's response to a massive hack of IT service provider SolarWinds. Oliver Contreras / Pool via CNP / SplashNews/Newscom

The Biden administration is preparing a new set of actions to improve cybersecurity defenses after the massive hack of IT services provider SolarWinds Inc. exposed vulnerabilities in U.S. critical infrastructure, a top National Security Council official said Friday.

But as the White House looks to deal with one hacking crisis, another, perhaps larger breach of Microsoft Corp.'s widely used email servers poses a new test for President Biden's cybersecurity policies.

Anne Neuberger, deputy national security adviser for cyber and emerging tech, said Biden is planning to unveil an executive action that aims at "building standards for software, particularly software that's used in critical areas."

The executive order is in response to the massive Russian-linked espionage campaign that has affected nine agencies and around 100 organizations by exploiting a commonly used software product from Austin-based SolarWinds.

The administration is also working on identifying and blocking "high impact activities" that focus on industrial control systems and operational technologies (OT) like those that manage the grid, Neuberger said.

"We have to be able to see and block malicious activity in critical industrial control system [ICS] networks across energy, gas, electricity, pipelines, water and chemical critical infrastructure sectors," Neuberger said.

She added that the executive order will tackle some of the lessons from the SolarWinds espionage campaign, such as the murkiness of many vital computer networks.

Neuberger said that "numerous sites across the industrial community, including power, water and manufacturing, were compromised at the ICS/OT network layer, where there was limited if any visibility of the problem."

She said the lack of insight into industrial networks "mitigates our ability to actually address the malware that could create system failures." Cybersecurity experts have long warned about the increasing number of internet-facing devices in the U.S. grid, which adds to the ways a hacker can infiltrate critical infrastructure.

Neuberger pointed to a recent compromise of a Florida water treatment system, when an attacker tried to poison the water supply of a small town by raising the levels of sodium hydroxide to over 100 times their normal concentrations (***Energywire***, Feb. 9). The attempted poisoning in Oldsmar, Fla., was only stopped because an operator happened to see the attacker move the mouse across the screen and change levels of the chemical. Neuberger said that detecting the attack was "not by means of cybersecurity, but rather serendipity."

"The level of trust we have in our systems has to be directly proportional to the visibility. and the level of visibility we need has to match the consequences of a system," Neuberger said.

She said the White House has been working with the Electricity Subsector Coordinating Council — a high-level group of utility CEOs and grid officials — as well as other groups in addressing OT security.

A National Security Council spokesperson declined to provide additional details on the upcoming actions.

A Department of Energy official told E&E News that the agency is "not aware of any energy sector entities" that have been targeted by the SolarWinds hackers after discovering the so-called Sunburst malware on their networks.

A 'terrifying' new hack

But as the Biden administration ramps up cybersecurity safeguards in response to SolarWinds, a possibly bigger espionage campaign is already underway. A recent "zero-day" flaw in Microsoft Exchange Servers — so called because it's previously unknown, so cyber defenders have had zero days to prepare for it — is reported to have been exploited by China-linked hackers. The severe vulnerability lets an attacker gain persistent access to the server as well as control over the business network, researchers say, and the attack has potentially hit thousands of organizations worldwide.

The vulnerability was initially used by the hacking group dubbed "Hafnium," according to a **blog post** from Microsoft on Tuesday. The group, which the tech giant said is "assessed to be state-sponsored and operating out of China," was targeting "infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs," the blog post noted. Since the software flaw was made public, there has been a dramatic increase in the number of criminal hackers seeking to take advantage of it before companies can fix the problem, researchers say.

The number of victims is likely to be as high as 30,000 in the United States, **wrote** cybersecurity journalist Brian Krebs, who first reported the extent of the breach. Former Cybersecurity and Infrastructure Security Agency Director Chris Krebs **said on Twitter** that the real impact could "dwarf" that number and that the "sheer scale & speed of this one is terrifying."

"This is a crazy and huge hack," Krebs wrote.

White House press secretary Jen Psaki said during a press briefing Friday that "this is a significant vulnerability that could have far-reaching impacts."

"First and foremost, this is an active threat," Psaki said. "We are concerned that there are a large number of victims and are working with our partners to understand the scope of this."

Last week, CISA, which is part of the Department of Homeland Security, issued an **emergency directive** requiring that federal agencies either immediately apply patches to fix the vulnerability or disconnect the Microsoft email server if it may have been compromised by hackers.

The North American Electric Reliability Corp. issued an all-points bulletin Wednesday about the compromise as well as an alert on Friday, a spokesperson said. The alert was an industry advisory that does not require electric utilities to respond, according to NERC, which oversees U.S. power grid security along with the Federal Energy Regulatory Commission.

FERC and DOE did not respond to requests for comment on the latest hacking campaign.

Twitter: **@chrismvasq** | Email: **cvasquez@eenews.net**