Source : www.thehindu.com Date : 2023-12-09

TOP WHITE HOUSE CYBER AIDE SAYS RECENT IRAN HACK ON WATER SYSTEM IS CALL TO TIGHTEN CYBERSECURITY

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

To enjoy additional benefits

CONNECT WITH US

December 09, 2023 09:56 am | Updated 09:56 am IST

COMMents

SHARE

READ LATER

FILE PHOTO: Miniatures of people with computers are seen in front of binary codes and words 'Cyber attack' in this illustration taken July 19, 2023. REUTERS/Dado Ruvic/Illustration/File Photo/File Photo | Photo Credit: Dado Ruvic

A top White House national security official said recent cyber attacks by Iranian hackers on U.S. water authorities — as well as a separate spate of ransomware attacks on the health care industry — should be seen as a call to action by utilities and industry to tighten cybersecurity.

Deputy national security adviser Anne Neuberger said in an interview on Friday that recent attacks on multiple American organisations by the Iranian hacker group “Cyber Av3ngers" were “unsophisticated” and had “minimal impact” on operations. But the attacks, Neuberger said, offered a fresh warning that American companies and operators of critical infrastructure “are facing persistent and capable cyber attacks from hostile countries and criminals” that are not going away.

“Some pretty basic practices would have made a big difference there,” said Neuberger, who serves as a top adviser to President Joe Biden on cyber and emerging technology issues. “We need to be locking our digital doors. There are significant criminal threats, as well as capable countries — but particularly criminal threats — that are costing our economy a lot.”

The hackers, who U.S. and Israeli officials said are tied to Tehran's Islamic Revolutionary Guard Corps, breached multiple organisations in several states including a small municipal water authority in the western Pennsylvania town of Aliquippa. The hackers said they were specifically targeting organisations that used programmable logic controllers made by the Israeli company Unitronics, commonly used by water and water treatment utilities.

(For top technology news of the day, subscribe to our tech newsletter Today’s Cache)

Matthew Mottes, the chairman of the Municipal Water Authority of Aliquippa, which discovered it had been hacked on Nov 25, said that federal officials had told him the same group also breached four other utilities and an aquarium.

The Aliquippa hack prompted workers to temporarily halt pumping in a remote station that regulates water pressure for two nearby towns, leading crews to switch to manual operation.

The hacks, which authorities said began on Nov. 22, come as already fraught tensions between the U.S. and Iran have been heightened by the two-month-old Israel-Hamas war. The White House said that Tehran has supported Houthi rebels in Yemen who have carried out attacks on commercial vessels and have threatened U.S. warships in the Red Sea.

Iran is the chief sponsor of both Hamas, the militant group which controls Gaza, as well as the Houthi rebels in Yemen.

The U.S. has said they have uncovered no information that Iran was directly involved in Hamas' Oct. 7 attack on Israel that triggered the massive retaliatory operation by Israeli Defense Forces in Gaza. But the Biden administration is increasingly voicing concern about Iran attempting to broaden the Israeli-Hamas conflict through proxy groups and publicly warned Tehran about the Houthi rebels' attacks.

“They’re the ones with their finger on the trigger,” White House national security adviser Jake Sullivan told reporters earlier this week. “But that gun — the weapons here are being supplied by Iran. And Iran, we believe, is the ultimate party responsible for this.”

Neuberger declined to comment on whether the recent cyber attack by the Iranian hacker group could portend more hacks by Tehran on U.S. infrastructure and companies. Still, she said the moment underscored the need to step up cybersecurity efforts.

The Iranian “Cyber Av3ngers” attack came after a federal appeals court decision in October prompted the EPA to rescind a rule that would have obliged U.S public water systems to include cybersecurity testing in their regular federally mandated audits. The rollback was triggered by a federal appeals court decision in a case brought by Missouri, Arkansas and Iowa, and joined by a water utility trade group.

Neuberger said that measures spelled out in the scrapped rule to beef up cybersecurity for water systems could have "identified vulnerabilities that were targeted in recent weeks.”

The administration, earlier this year, unveiled a wide-ranging cybersecurity plan that called for bolstering protections on critical sectors and making software companies legally liable when their products don’t meet basic standards.

Neuberger also noted recent criminal ransomware attacks that have devastated health care systems, arguing those attacks spotlight the need for government and industry to take steps to tighten cyber security.

A recent attack targeting Ardent Health Services prompted the health care chain that operates 30 hospitals in six states to divert patients from some of its emergency rooms to other hospitals while postponing certain elective procedures. Ardent said it was forced to take its network offline after the Nov 23 cyberattack.

A recent global study by the cybersecurity firm Sophos found nearly two-thirds of health care organizations were hit by ransomware attacks in the year ending in March, double the rate from two years earlier but dipping slightly from 2022.

“The president’s made it a priority. We’re pushing out actionable information. We’re pushing out advice,” Neuberger said. “And we really need the partnership of state and local governments and of companies who are operating critical services to take and implement that advice quickly.”

COMMents

SHARE

technology (general) / cyber crime

BACK TO TOP

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com

crackIAS