Related news

cyberscoop.com/israel-cyberattacks-water-iran-yigal-unna/

May 28, 2020

government

Israeli official confirms attempted cyberattack on water systems

Israeli cyber chief Yigal Unna (ICT).
Written by Sean Lyngaas
May 28, 2020 | CYBERSCOOP
Israel last month thwarted a cyberattack on control systems at water facilities, a senior government official said Thursday while warning of the dangers of escalating conflicts in cyberspace.

The “synchronized and organized attack” on civilian infrastructure was aimed at disrupting the industrial computers that underpin Israeli water facilities, said Yigal Unna, head of Israel’s National Cyber Directorate, in the most extensive public comments from an Israeli official yet on the incident. Damage could have been done to those systems if Israeli authorities hadn’t foiled the attack, Unna claimed.

“We’re now in the middle of preparing for the next phase [of attacks] to come — because it will come eventually,” he said in a speech streamed at the CybertechLive Asia conference.

Public details on the attack are scarce, as Israeli officials have not released forensic data in connection with the incident. The Israeli cyber directorate issued a terse statement in late April about attempted breaches of water pumping stations and treatment plants, and urged companies in the sector to take defensive measures.

Multiple media reports blamed Iran for the malicious activity. (CyberScoop could not independently confirm this attribution.) The Iranian government has denied involvement.

Unna acknowledged the suggestions, but did not specifically blame Iran.

“We are not attributing or saying anything officially about who’s behind it,” he said. “But it’s not a gang, it’s not a cybercrime group. They gain nothing from it.”

In retaliation, Israeli hackers breached computers at an Iranian shipping port in early May, according to a Washington Post report.

After mentioning that report, Unna suggested that Israel may have hit back at Iran for the cyberattack. “Maybe and maybe not,” he said. “It seems like there are new rules of engagement, rules of war” in cyberspace.

Galina Antova, co-founder of industrial cybersecurity company Claroty, said the attempted cyberattack on Israeli water systems “highlights that while water infrastructure typically eludes the public’s attention as a major source of cyber risk, it remains susceptible to both targeted and non-targeted threats.”

Israel and Iran — two bitter enemies — have long conducted cyber-operations against each other as part of a broader regional conflict. More than a decade ago, suspected U.S. and Israeli intelligence operatives used the Stuxnet computer worm to sabotage centrifuges at an Iranian nuclear facility.

The coronavirus pandemic has reaffirmed that hackers are unwilling to refrain from attacking critical infrastructure, Unna said.

Red lines will continue to be crossed, he said, referring to recent cyberattacks on the Czech health care sector. “Cyber winter is coming and coming faster than even I suspected.”