Analysis-Mexico data hack exposes government cybersecurity vulnerability

By Diego Oré

Published: 2022-10-01 · Archived: 2026-04-06 15:26:19 UTC

Diego Oré

October 1, 2022 2 min read

By Diego Oré

MEXICO CITY - A major hack into classified government information in Mexico, including thousands of emails from the armed forces, exposed the country's vulnerability to cyberattacks due to under-investment and poor technological preparedness, experts said on Friday.

President Andres Manuel Lopez Obrador confirmed on Friday the Defense Ministry had suffered a hack that revealed details about his heart condition - a form of angina - as well as information on criminal figures, transcripts of communications, and the monitoring of the U.S. ambassador to Mexico.

A group called "Guacamaya" - or "macaw" in Spanish - claimed responsibility for the hack and said on its website it had accessed six terabytes of data.

The size of the hack suggested prior planning, said Francisco Solano, an executive at IT services and consulting firm Logicalis.

"This did not happen by chance," he said.

According to Solano and other analysts consulted by Reuters, the vulnerability exploited by the hackers stemmed from a weakness in a Microsoft server detected last year, known as ProxyShell.

Although solutions to fix the problem were available, the government needed to carry out updates to implement them.

"You have the antidote, but nobody to apply it," Solano said, adding that there appeared to be a lack of resources to resolve the issue.

Microsoft did not immediately respond to an emailed request for comment.

On Friday, at his daily news conference, Lopez Obrador said that hackers had exploited a change in the military's IT systems, without giving further details.

The armed forces did not respond to a request for comment.

Governments worldwide have been increasingly targeted by aggressive cyber crime in recent years and have been forced to increase investment and focus on cybersecurity.

In Latin America, Mexico ranks as the country most targeted by cyberattacks in public and private sectors combined, several studies have shown.

Mexican oil company Pemex, National Lottery and National Transparency Platform have been hit by cyberattacks in recent years.

Although Mexico's government has steadily devoted more resources to cybersecurity, the investment is not enough compared to what is needed to ward off attacks, experts said.

Hackers would have needed up to three days to copy the information, said Adolfo Grego, a forensic specialist, also raising questions over why the government did not act sooner.

(Reporting by Diego Oré; Editing by Muralikumar Anantharaman)
