Source: https://www.govtech.com/security/virginia-legislative-systems-disrupted-by-ransomware-attack

CYBERSECURITY

Virginia Legislative Systems Disrupted by Ransomware Attack

Several of the systems used by state lawmakers have been taken offline following a cyber-attack against the Division of Legislative Automated Systems. The attack comes just a month before the next legislative session.

December 14, 2021 •

Shutterstock

A ransomware attack has disrupted key systems used by Virginian legislators.

The attack hit the legislative branch's IT agency, the Division of Legislative Automated Systems (DLAS), impacting all of its servers, according to an email obtained by the Associated Press from Executive Director Dave Burhop. The attack downed a variety of services, including the digital system that legislators use for drafting bills.

The breach strikes only a month before the General Assembly is scheduled to reconvene for a legislative session beginning in mid-January.

The incident also took offline the budgeting portal and more general services, such as the legislative branch's voicemail system, per the email.

The Virginia Law Portal, which enables online reading of the state code and constitution, and the Virginia Capitol Police's website were also downed, per *The Washington Post*. The rest of the Capitol Police's systems are reportedly unscathed, however.

The attack is "very impactful" and prevents DLAS from accessing "most of their critical

systems," Alena Yarmosky, a spokesperson for Gov. Ralph Northam, reportedly said in a written statement. She said DLAS shut down most of its servers to contain the malware's spread, and that the state's Fusion Center issued an email about the attack late Sunday night.

Burhop's email said that hackers left a ransom note that did not specify the extortion price or date.

The attack did not reach the executive branch, and by Monday, Gov. Northam had instructed executive agencies with the capabilities to aid in the response. Virginia also is turning to the help of cybersecurity firm Mandiant, which it engaged earlier this year following another incident.