CYBERSECURITY

Cyberattack Afflicts Minnesota State Senate Computers

The Minnesota state Senate's servers were breached Tuesday morning, and the hackers were able to access a file of passwords used by senators and staff, Senate officials said Tuesday evening.

June 03, 2020 • Dave Orrick, Pioneer Press

Shutterstock/NicoElNino

(TNS) — The Minnesota Senate's servers were breached Tuesday morning, and hackers were able to access a file of passwords used by senators and staff, Senate officials said Tuesday evening.

The breach prompted the Senate's information services to quickly take down the Senate's website and begin slowly rebuilding pages. As of 6 p.m., a number of Senate web pages were still down.

The attack succeeded early Tuesday morning, according to a letter sent Tuesday evening to senators and staff from Secretary of the Senate Cal Ludeman.

It's not clear if the Senate attack is connected to a [different set of cyber attacks](#) being launched on state computers that officials revealed Sunday. Those attacks — [distributed denial of service attacks](#) — are ongoing and have led to occasional outages on some state web pages. However, they don't involve anyone gaining access inside any state systems, a

spokeswoman for MNIT, the state's information technology agency, said Tuesday evening.

Here's part of Ludeman's letter:

"At 4:24 this morning, the Senate server was hacked and accessed for several minutes. … SIS (Senate Information Services) brought down the server as a precaution and, with the help of MNIT and the FBI, they have been able to trace what was accessed within the server, namely the Passwords File.

"The Passwords File that was accessed as well as passwords to our main database server have all been reset and log files checked to assure there is no further unauthorized access to the servers. These passwords also included the Senate WiFi password. As a result, the Senate WiFi network was brought down to reset and test as another precaution. This Passwords File does NOT contain passwords to Senator or staff emails or login accounts, nor does it have access to the server that has that information. The original website breach caused SIS staff to slowly rebuild pages as they confirmed them to be secure. This will be an ongoing process … ."