TechXplore

Hacked software provider won't say if ransomware involved

September 25 2020, by Frank Bajak and Jake Bleiberg

The sign for Tyler Technologies is seen outside the company's offices, Thursday, Sept. 24, 2020, in Plano, Texas. The major U.S. provider of software services to state and local governments, including the online publishing of election results, has told customers that an unknown intruder broke into its phone and IT systems. Plano, Texas-based Tyler Technologies told customers in an email that it discovered the breach and contacted law enforcement and enlisted outside cybersecurity help. (AP Photo/LM Otero)

A day after informing customers that it had been hacked by an unknown intruder, a major U.S. provider of software services to state and local governments —including posting election data online— said the impact appeared limited and there is no reason to believe its customers were affected.

Tyler Technologies' profit-seeking ransomware purveyors.

Customers' use of Tyler products for election data reporting appears limited.

Nashville's information technology director said the city uses a Tyler "open-data" product, Socrata, to post unofficial election night results, among other uses. A spokeswoman for Ramsey County, Minnesota's second-largest, which includes the state capital of St. Paul, said it uses Socrata to report election results but does not post them until they have been certified. In both instances, the data comes from separate election authorities.

Tyler said Socrata data is hosted on Amazon Web Services, not on the network that was hacked.

The publicly traded S&P 500 company, provides software services for everything from jail and court management systems to payroll, human resources, tax and bill collection and land records. It also serves schools. Tyler says it has 5,500 employees and 1,500 customers in all 50 states and abroad.

A cybersecurity expert assisting municipalities that are Tyler customers, Mike Hamilton of CI Security, said he was concerned hackers may have obtained access to customers' passwords stored on its network and could penetrate their systems. Hamilton, a former chief information security officer for Seattle, said Tyler should be notifying customers to immediately reset all their passwords as a precaution.

"It's completely possible that bad guys have been in there for a good amount of time," he said.

The sign for Tyler Technologies is seen outside the company's offices, Thursday, Sept. 24, 2020, in Plano, Texas. The major U.S. provider of software services to state and local governments, including the online publishing of election results, has told customers that an unknown intruder broke into its phone and IT systems. Plano, Texas-based Tyler Technologies told customers in an email that it discovered the breach and contacted law enforcement and enlisted outside cybersecurity help. (AP Photo/LM Otero)

Ramsey County spokeswoman, Allison Winters, said the Socrata platform is hosted remotely "and is entirely web based." She said it does not, however, employ two-factor authentication for logging in by county employees— a serious cybersecurity deficiency that makes stealing log-in credentials easier.

Hamilton said Tyler's major product for municipalities, Munis, also lacks two-factor authentication.

Cybersecurity analysts speculated that Tyler was hit by ransomware, whose purveyors are increasingly breaking into company and government networks and siphoning out valuable data before scrambling them and demanding payouts. They threaten to make the stolen data public if the victim doesn't pay up.

Brett Callow, an analyst with the cybersecurity firm Emsisoft, said Tyler may have been hit with the same ransomware that struck the Texas Department of Transportation, based on an encrypted file uploaded to the Google-owned malware identification service VirusTotal in June that included "tylertech" in the file name.

Data breaches often are not discovered until months after the fact, or until data is suddenly scrambled and a ransom demand issued.

Hanna Pickering, director of information technology in Portland, Maine, said the city uses Tyler platforms for payroll, permitting, city inspections, city planning and human resources, among other things. Those city functions have not been affected by the breach at Tyler, she said.

Pickering said she'd be more concerned if Tyler hosted the city's information, but in Portland "our network protects our data."

Citation: Hacked software provider won't say if ransomware involved (2020, September 25) retrieved 20 April 2024 from https://techxplore.com/news/2020-09-hacked-software-wont-ransomware-involved.html