Massachusetts cities, towns warned of potential server infiltration

By Colin A. Young
State House News Service

The state's cybersecurity chief warned municipal leaders of a high-risk threat to a common email system over the weekend as federal officials urge businesses and governments to protect themselves against what the White House said is "a significant vulnerability that could have far-reaching impacts."

Secretary of Technology Services and Security Curt Wood sent an alert to local leaders Saturday to make sure cities and towns in Massachusetts that use an on-site Microsoft Exchange server were aware that state-sponsored hackers from China have been able to infiltrate the servers to steal emails, address books and other information.

"You should take immediate and appropriate action to protect your environment," Wood wrote, directing local leaders to a bulletin published by the Multi-State Information Sharing and Analysis Center and an emergency directive from the U.S. Cybersecurity and Infrastructure Security Agency.

White House spokeswoman Jen Psaki said Friday the Microsoft breach "is an active threat" and that the Biden administration is "concerned that there are a large number of victims." Independent cybersecurity journalist Brian Krebs reported Friday that the hack had affected "[a]t least 30,000 organizations across the United States – including a significant number of small businesses, towns, cities and local governments."

The Executive Office of Technology Services and Security was not able to provide updated information Monday morning, and the Massachusetts Municipal Association was not immediately available to discuss the potential impact on cities and towns in Massachusetts.

Microsoft’s Threat Intelligence Center said the group behind the hack is HAFNIUM, a state-sponsored cyber unit that the company said “primarily targets entities in the United States across a number of industry sectors, including infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and NGOs.”

Cybersecurity has been a point of increasing emphasis for state and municipal officials in recent years because of the widespread shift to doing business over the internet and incidents in which cybercriminals have sought to extort cities and towns by inappropriately gaining access to municipal files, like the 2019 ransomware attack on New Bedford.

Gov. Charlie Baker pushed information technology and cybersecurity closer to the forefront of state government in recent years by creating the Cabinet-level Executive Office of Technology Services and Security in 2017 and pushing for the creation of the MassCyberCenter in 2018 to bolster the state’s cybersecurity readiness and to promote the cybersecurity economy.

Last fall, as hospitals were shoring up their cyberdefenses to protect themselves against a wave of ransomware attacks on health care facilities, Baker highlighted ransomware attacks — in which hackers gain access to important information and hold it ransom from the rightful owners — as “a persistent threat to municipalities.” The MassCyberCenter works with communities to provide assistance in developing or reviewing cyber incident response plans.

Cybercrime is also a threat to individuals. Review site Safety.com said last year that Massachusetts ranked 10th among states in terms of the financial impact of cyber incidents. Using data from the 2019 FBI Internet Crime Report, the site found that Massachusetts residents lost almost $84.2 million to cybercriminals in 2019 and that the average loss of $12,966 per victim was the fourth highest in the nation.

Late last year, Wood and EOTSS dealt with the SolarWinds hack, which federal officials said posed “a grave risk to the Federal Government and state, local, tribal, and territorial governments as well as critical infrastructure entities and other private sector organizations.” Wood said at the time that there were no signs that state government systems had been compromised.

In 2019, Wood told lawmakers that the state’s computer network is “probed” more than half a billion times each and every day by entities outside the United States looking for a weak spot in the state’s cyber protections that could allow bad actors to infiltrate the state’s information technology infrastructure.

“Every day, we have attacks. Just to give you a frame of reference, we have implemented new technology in the state where we are kind of able to analyze everything that comes into the state network and I will say as of today on a daily basis we receive about 525 million probes a day from foreign soil,” Wood said in September 2019. “They’re pinging our network, they’re scanning our commonwealth network trying to find a vulnerability.”