Video Conferencing Concerns Prompt Government Focus on Remote Cybersecurity

Vulnerabilities lead to questions about home networks and "bring-your-own-device" policies.

James Mersol

Wed, 04/22/2020 - 11:57

Photo Credit: mikkelwilliam/iStock

While organizations at all levels of the public, private and nonprofit sectors adjust procedures for a long-term telework scenario, security issues stemming from popular video-teleconferencing platform Zoom have led these organizations to not only consider how to best safeguard this necessary communication technology, but also its role in the broader remote security landscape.

The rise in Zoom's popularity coupled with user error on setting up VTC access has led to the phenomenon of "zoom-bombing," where unauthorized users access calls and harass participants with pornography, hate speech and threatening language. User groups including virtual school classrooms and Congress have fallen victim to the tactic.

House Oversight Committee Ranking Member Jim Jordan cited an April 3 hearing with the Special Inspector General for Afghanistan Reconstruction (SIGAR) that was zoom-bombed "at least three times," in an April 10 letter asking Committee Chairwoman Carolyn Maloney to suspend use of the platform. The Senate has discontinued using Zoom over similar concerns.

The primary concern security professionals have raised over Zoom is not the proliferation of this "Zoom-bombing," but the inherent security flaws in the program itself. As the Los Angeles Times reported last week, Zoom is working to fix a number of vulnerabilities in its platform, including flaws that allowed hackers to remotely access users' webcams and install software without users' permission. There is no evidence that Zoom itself has abused these flaws, but they are severe enough that several organizations have banned the platform, fearing that malicious actors could use them as a vector to compromise an entire network.

In an April 9 agency memo, Immigration and Customs Enforcement (ICE) CIO Rachelle Henderson asked all of the agency's employees and contractors to avoid installing Zoom software on agency equipment, recognizing the vulnerability in the software. However, Henderson said accepting outside Zoom requests is permissible, as long as they do not install Zoom software locally and avoid sharing any sensitive information.

The distinction between agency devices and personal devices is critical as many public- and private-sector organizations have adapted their "bring-your-own-device" (BYOD) policies for work during the COVID-19 pandemic, an adaptation that some predict will have effects even once employees are able to return to the office.

"BYOD is now the reality, and it will continue to be," said Greg Touhill, former federal CISO and president of mobile security firm AppGate Federal Group, "because I don't think we're going back."

Given the shift to telework, adversaries now look at home networks and personal devices as the weak links that will give them access to sensitive networks, Touhill said. Few employees are likely to have the same level of home network security that their cybersecurity teams have implemented at the office, and even those who do are often reluctant to give CISOs visibility into their personal devices.

Before looking into endpoint security solutions, one solution organizations can focus on is creating baseline principles for security and monitoring which devices are on the network, a principle of the federal continuous diagnostics and mitigation (CDM) program.

Elsewhere, organizations are seeing that “early investments in zero trust [are] paying off,” according to Touhill. Government agencies that have focused on the identity-based model of security have encountered fewer technical hurdles to access as the shift to telework enters the medium and long term.

The best solution for agencies who want to use Zoom and are mindful of these concerns is to use Zoom for Government, a FedRAMP-approved version of the software. The Cybersecurity and Infrastructure Security Agency (CISA) and the General Services Administration (GSA) recommended the platform for agencies in a joint statement earlier this month. Despite the same name, provider and front-end experience, Zoom for Government is housed on a separate cloud server than the commercial version.

Although neither Zoom nor the agencies it serves have publicly disclosed specific use cases, Zoom's website explains that agencies including the departments of Homeland Security and Energy and the Centers for Disease Control and Prevention use Zoom for Government not only for intra-agency communication, but also as an enabler for emergency services and telehealth.

For agencies and organizations without access to Zoom for Government, special agents working for the FBI’s Computer Intrusion Program recommended that everyone pick the video teleconferencing platform that works best for them, weighing concerns over privacy, vulnerabilities and user accessibility. Each platform has had vulnerabilities, they explained, but users can make informed decisions based on how responsive and transparent the company was about the issue.

For broader concerns over home network security, the special agents recommended that users follow cyber hygiene principles, including having a heightened awareness of phishing, especially related to COVID-19, and regularly patching systems and software.

For home networks, practical risk mitigation measures include using WPA2 or WPA3 encryption, changing default passwords and updating router firmware. Because many routers offer multiple networks — typically described as a home network and a “guest network” — another solution is to segment the network, keeping sensitive traffic to one of the two networks and restricting all other devices to the other network.

View printer friendly version
coronavirus
Federal Cybersecurity
mobile security
Zero Trust
Federal Government Telework
Standard