Assessing Risk in Video Conferencing Solutions

David Rossell, Director of Security and Consulting Services

Executive Summary

Clients should feel comfortable using Zoom for all public meetings. There has been much coverage in the press about security and privacy concerns surrounding the use of the Zoom video conferencing product and several high-profile organizations have forbidden its use. These concerns are valid for especially sensitive conversations such as those related to government, defense, or intelligence matters. They also are valid for meetings in the defense industrial base or other sectors that are prominent targets for industrial espionage. Aside from these specific cases, employing Zoom for video conferencing presents a relatively low risk.

Zoom and Chinese Ownership

Zoom is a publicly traded company on the NASDQ exchange. Its CEO, Eric Yuan, was born in China, and emigrated to the United States in the late 1990s. He lives in California and according to Forbes is an American citizen. Yuan was instrumental in the creation of Cisco's WebEx product.

Privacy Risks

Zoom has been forced to address several privacy missteps that have come to light during the COVID crisis. It has removed a feature that allowed a meeting host to determine the "attention" level of attendees; it also removed an integration with Facebook that disclosed Zoom user data to Facebook. As with other video conferencing solutions, public Zoom meetings are at risk of "meeting bombing," that is, unwanted attendees disrupting the meeting. With all video conferencing solutions, this risk can be mitigated by requiring passcodes and appropriate configuration of the meeting, such as blocking audio and video of public attendees when they join and controlling access to the Q&A and chat features. Zoom, like other conferencing solutions, allows meetings to be recorded.

Security Risks

All video conference solutions implement some degree of encryption that safeguards data from unauthorized viewing as it traverses the Internet. In most situations with most providers, this data is decrypted (made readable) at some point within the provider's infrastructure unless specific features are enabled. Decrypted data is theoretically open to view, raising the concern that Zoom and other providers can "spy" on conference content. Zoom has come under specific attack for poor implementation of a standard encryption framework, and its encryption should not be regarded as secure from attack by nation-state or large commercial or criminal organizations. This is not a concern with other video conferencing products.

Risk Management

Employ Microsoft Teams for internal video calls. Extremely sensitive information should be conveyed via telephone or a secure messaging application such as FaceTime, WhatsApp, or iMessage (when both users have iPhones). Video conferences for public events or calls requiring basic confidentiality controls can leverage whatever solution is simplest – including Zoom - and most usable from a participant perspective. With all video conferencing solutions, you should make sure you use the most up-to-date version of the software. This is a good rule of thumb for any software in your organization.