Whitepaper

Security for government contractors

webex by CISCO

© 2021 Cisco and/or its affiliates. All rights reserved.

Hackers are finding new ways to access government information.

Are you a target?

You may think of hackers stealing information from databases and corporate accounts. In reality, hackers can tap into both stored and in-transit content and communications to steal information about government projects, including your calls, messages, and meetings. A good example is when in June 2021 a large defense contractor had their technical support department hacked by a foreign group with the intent to access and intercept U. S. government communications. These groups are attempting to access information through government contractors who may not have the protection needed to prevent these security breaches. It is important for all government communication to have protection against any intruders.

Outsiders may be trying to intercept your communications with the government

Can your communications be recorded by outsiders?

You should not overlook securing your meetings, messages and conversations when planning your infrastructure. Hackers can act as a meeting participant joining meetings without your knowledge. Intruders can tap into phone calls recording sensitive conversations. Messages can be intercepted stealing private information. You may never know they are there until the government finds the source of the information leak. This may result in cancellations of your government contracts and huge fines.

Are your meetings and messages open to the public?

Public internet clouds allow access to users from anywhere in the world. Man-in-the-middle attacks, where communication is leaked from the internet, are becoming common for services without proper security. Some communication service providers route traffic through data centers in other countries where it could be intercepted by foreign governments or hackers. Without appropriate protection, your conversations can be accessed through public clouds.

Additionally, hackers can access your employees' cell phones through common smart phone apps. Employees using a personal app on their phone can mistakenly expose business information without knowing. Malware can enter through cell phones and destroy files and apps. Rogue employees or those who have left the company may have sensitive information on their cell phones that needs to be removed. Mobile protection must prevent access to business and government applications and remotely delete files and business applications after an employee leaves the company.

What you need to know now to protect sensitive communications

Collaboration and conferencing services should have encryption, which is an encoding of your conversations. However, if the encryption is done in the cloud or in only part of the network, then the information is still susceptible to hackers. Some messaging systems have end-to-end encryption, where the encryption starts at the user's device and is decoded at all participants' devices. End to end encryption is important but may also be susceptible to intruders if the encoding keys are stolen by someone listening on the network. Encryption

© 2021 Cisco and/or its affiliates. All rights reserved.

alone is not the answer. You must be able to verify each attendee in your meetings.

When communicating with your associates in other companies, it is important to know their security policies. These policies may be vastly different from your company's policies, opening avenues for security breaches. Collaborating with an outside company requires you to bring them into your secure government authorized environment. Some services require you to purchase licenses for all guests outside your company creating an expensive and difficult to manage scenario. The best solution is to have a service provider who can bring your guests into your FedRAMP system and allow collaboration with your security policies, always keeping information within the FedRAMP system. When working with outside organizations be certain that messaging and meetings are secure both inside and outside your corporation.

How you can be protected now

1. Zero trust security

Implementing protocols that verify user identities is crucial to preventing imposters in your meetings. Zero Trust Security is a standardized method for showing hosts that their attendees are authorized to attend. This protocol verifies users through passwords and displays a visible key confirming intended participants. Additionally, Zero Trust Security provides end to end encryption where the encryption keys are generated by the host not in the network. These keys cannot be stolen within the network and only the verified users are allowed to see the meeting content. Cloud services, or any operations in the cloud, are incapable of mounting passive attacks on conversations by ensuring that user-generated content (UGC) is encrypted end-to-end with keys that are not exposed to the conveying cloud services. Zero Trust Security provides a very strong defense against impersonation and network attacks.

2. Data loss prevention

With real-time DLP, you can prohibit classified content from ever being sent, rather than redacting or deleting content after it is posted. A DLP engine scans content generated by users and identifies and provides visibility into policy violations. It is imperative that DLP policy engines support a rich set of pre-defined policies across industry verticals such as finance (routing number, bank account number), healthcare (PII, drug name), education (student loan information, FERPA), and many more that result in the most common data compromise scenarios.

3. Anti-Malware

Anti-Malware protects users from malicious files and URLs. It follows users even when they are collaborating outside of company boundaries or when malicious files and URLS are introduced by users beyond the company security system.

© 2021 Cisco and/or its affiliates. All rights reserved.

4. FedRAMP internal and external to your corporation

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. If your communication with government agencies requires FedRAMP authorization, be certain that all external communications are protected by the required security. Having conversations with organizations not employing a FedRAMP system can expose you to threats and risks. Be certain that your security policies incorporate all guests and external communications.

5. Department of Defense (DOD) IL5 certification and DFARS, ITAR and NIST compliance

If your communication is with the Department of Defense, you will need to be compliant with a few regulations. DFARS protects the information used by DOD suppliers. ITAR regulates the import and export of defense materials and the documentation surrounding them. NIST, the National Institute of Standards and Technology, has several policies that protect communications. IL5 is required if you need access to the private NIPRNet network. As you evaluate communication services, be aware of which standards they comply with.

6. Device and end user security

An organization that would like to support a bring your own device (BYOD) environment usually requires containerization of enterprise applications, separating personal apps from business apps. This requires mobile application management (MAM) software to secure mobile apps. With this software you can publish, push, configure, secure, monitor, and update mobile apps for your users and more safely onboard users to your collaboration apps in a manner that meets your enterprise compliance requirements. Mobile phone protection software is necessary to isolate personal apps from business information and erase sensitive information when an employee no longer works for your company.

7. Multifactor authentication (MFA)

Most people today use fewer than five passwords across their different Internet sites, allowing attackers the ability to replay passwords from compromised sites in other accounts until they find a site where that password has been reused. MFA requires a secondary authentication either through a cell phone, email or input of an additional security key verifying the user or attendee to your meeting.

8. Compliance and certifications

Depending on the government agency you are working with, you may need to meet specific regulations and certifications. Be sure your communication and collaboration suppliers can meet FedRAMP, DFARS, FIPS 140-2, DOD Impact level and CMMC requirements.

9. The Cybersecurity Maturity Model Certification (CMMC)

CMMC is a training, certification, and third-party assessment program of cybersecurity in the United States government defense industrial base aimed at measuring the maturity of an organization's cybersecurity processes. It is important that personally managed devices have the same security as corporate devices. The CMMC framework consists of maturity processes and practices derived from multiple cybersecurity standards—primarily from NIST SP 800-171. The CMMC framework includes a comprehensive 3rd Party certification requirement to verify the implementation of processes and practices with the associated maturity level. In the future, this certification will be required to do work in support of the U.S. Department of Defense and potentially other government agencies. When choosing a communication and collaboration provider, be sure they can provide you with the necessary features, policies, and documentation to help you efficiently achieve CMMC certification.

10. Choose the right partners

Sometimes meeting standards and creating security policies can be overwhelming. Consultants may create difficult procedures or extensive implementation projects. Partnering with Webex by Cisco, the leader in collaboration security and government communication gives you the knowledge and support you need to achieve successful interactions with your government customers. Webex for Government has FedRAMP moderate authorization. Webex for Defense has Impact level 5 (IL5) authorization for achieving active work with the Department of Defense. This platform makes use of the NIPRNet Defense network to communicate with the DOD.

Why Webex?

Not all clouds are created equal

Even though a service provider is FedRAMP authorized, they may not have the security you need to lower your risks. The following blog describes how Webex exceeds the certifications to provide a better service (https://blog.webex.com/video-conferencing/webex-ranks-best-of-breed-in-nsa-collaboration-services-guidelines). The National Security Agency (NSA) published a set of guidelines for “Selecting and Safely Using Collaboration Services for Telework.” The guidelines that evaluated 17 collaboration service providers identified a dozen critical criteria for cybersecurity functionality and security assurance to help government employees and organizations make informed decisions when selecting a collaboration service for their needs.

Superior commitment

Cisco is committed to providing the best collaboration solution for the U.S. Department of Defense, and U.S. Defense Industrial customers. This includes delivering the required CMMC Level 3 compliance so that our solutions can be confidently used by Defense Industrial base (DIB) customers with the Department of Defense. To demonstrate this commitment Cisco has completed the self-assessment of the CMMC Level 3 controls. At the time of this publication, 3rd party auditors (3PAO) are awaiting DOD’s updated guidance on FedRAMP and CMMC reciprocity. Cisco Webex for Government will be audited by 3PAO upon availability of this guidance.

Consult the experts

When carefully considering collaboration cloud services, be certain that they can provide you with the highest level of security, management and support. Only Webex provides all of the capabilities listed in this paper. Choose Webex and you can have confidence that your communications are secure and meet government requirements.

For more information
Please contact Webex Sales

October 2021

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)