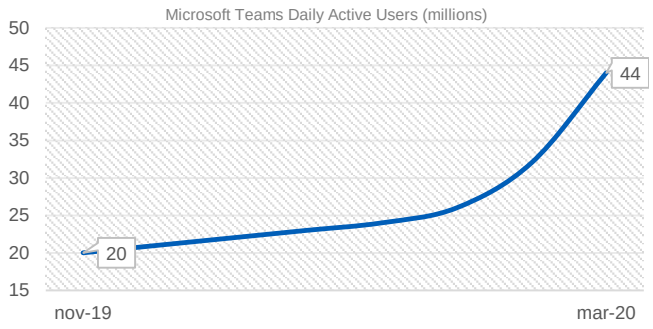
Secure Collaboration and Conferencing

16 April 2020

In the wake of the current crisis many businesses are finding themselves with a remote workforce and new ways of working. Collaboration tools can be an efficient way to keep teams connected and operating effectively. However, they also open the business to new potential risks.

While the usage of video conferencing tools was already on the rise, lockdowns instituted all over the world have accelerated this trend. In 2019, Gartner predicted that by 2024 around 75% of enterprise meetings would take place virtually, whereas in the current situation we recognise that we are already above this number. The number of daily active users of Microsoft Teams, for example, has more than doubled from 20 million in November 2019 to 44 million in March 2020.



For businesses, this can bring a variety of challenges, not only to the way of working, but also with regard to the security of company data. We see that businesses struggle to keep up with the often urgent demands from their workforce for remote working solutions, while still ensuring their security.

Most common risks

- **Data breaches**: A data breach is a security incident which occurs when information is disclosed, accidently or on purpose, to an unauthorised audience. With collaboration tools this can happen if access to work spaces is not appropriately managed or files can be easily shared and downloaded. It could also occur if screen sharing is enabled and private documents are displayed. A breach could expose business critical information, or even result in a fine under the GDPR if personal information were disclosed. Furthermore, with the ease of setting up a meeting come risks. When the meeting space has not been configured properly, it could be that unauthorised people get access to the meeting. Especially in meetings with many attendees this could pose a risk, as they will probably go unnoticed.
- **Overloading of the network**: With the increase of video conferencing usage, this puts additional demands on the bandwidth of the network. This is especially the case when a large number of employees are running video meetings through the company servers or over a company VPN. This could result is inaccessible files or meetings breaking up.

Out of the shadows – managing Shadow IT

Cloud services, including collaboration tools, can be used relatively easily for business purposes, without the approval or knowledge of IT, security or procurement. Employees are able to create (paid) accounts, without informing their organisation, and with the possibility to share confidential information outside of the organisation. This could lead to situations in which sensitive documents are stored in a cloud environment, without the organisation knowing about it and without the desired degree of security and control. This use of technology is often referred to as Shadow IT.

Most employees, especially in a time of uncertainty, are looking to continue delivering as effectively as possible. In the absence of clear guidelines, or viable alternatives, employees may take solution choice into their own hands.

While many of the risks remain the same, they are magnified due to the lack of oversight.

Tips for secure collaboration while working from home
While there are common risks, there are also common principles for ensuring the secure use of collaboration tools. Below, we have gathered some of the good practices, both in general and some examples for the most popular conferencing tools, to ensure secure collaboration.

General tips
While some settings and tips may be specific for a particular tool, there are some overlaps. In general:
- ensure that the conferencing software is enabled to encrypt the data that is sent across the network (in-transit), and preferably end-to-end;
- enable the use of a VPN is enforced for unencrypted network traffic;
- keep your conferencing tool up-to-date;
- consider lowering the video quality (e.g. 240p/360p/480p) to prevent overloading of the network;
- enforce multi-factor authentication across devices and applications.

Microsoft Teams
Microsoft Teams comes with a set of default security configurations to protect the end users and their data while in transport and at rest. Although, it is good to check if these security settings are enabled. Below we share with you multiple security configurations that can be checked/enabled:
- Modern Authentication (MA): is a method of identity management that offers more secure user authentication and authorisation. This feature is enabled by default.
- Multi-Factor Authentication (MFA): is an authentication method in which a user is granted access only after successfully passing two or more authentication methods which includes OTP, Tokens, SMS code, etc.
- Single-Sign-On SSO: single sign-on adds security and convenience when users sign on to applications. Although, to enable this feature you are required to have your users registered in either Azure Active Directory (Azure AD) or Hybrid Azure AD.

Because Teams is more than a conferencing tool, it is important to educate employees on the way they share files via this platform. For example:
- not to share confidential files in channels with guest users and use Microsoft Azure Information Protection (with DLP) for more security and control;
- making sure that there is no hidden access to files via the underlying SharePoint site;
- use a lobby when having a meeting with external users.

Cisco WebEx
Within Cisco WebEx there are many security items to configure. While some of these settings are enabled by default, it is preferable to go through them to ensure optimal security for your employees.
Based on Cisco's good practices, we recommend you have the below features enabled:
- Authenticated image files
- Encryption of data at rest and in transit
- Secure software development using Cisco's Secure Development Lifecycle (CSDL)
- Controlled security feature implementation using Cisco's Product Security Baselines (PSB)
- User authorisation using OAuth2
- Security and compliance features configured in Webex Control Hub, the Webex Teams' administrative portal.

Zoom Meetings
With a lot of customisation comes the potential for security errors. Find a list of good practices below:
- enforce passwords on all meetings;
- enable the waiting room to prevent unknown participants from joining;
- enable *wait for host to join* to ensure that only invited participants join;
- once all attendees are present, lock the virtual room;
- only allow registered or domain verified users in the meeting;
- don't use a personal meeting ID for public meetings.

Zoom has recently been challenged with security and privacy concerns. The results of investigations and future changes should be considered to determine its use.

Managing shadow IT
It is important to note that these are all tips to ensure secure working with a tool that has been sanctioned by the organisation. As discussed, the use of shadow IT by employees in the organisation could still pose a risk. One of the most important measures against this is using a Cloud App Security Broker (CASB). With a CASB it is possible to detect the usage of unauthorised conferencing tools and configure security measures to prevent this.

When using a CASB, it is important to first understand why employees are using the tools they are using. While blocking the tool could seem like an easy solution, this could cause other shadow IT to pop up. We would advise to:
- configure a CASB to discover what tools are used most;
- discuss with your employees why they use these tools;
- determine actions based on these outcomes.

The actions could vary from education on the capabilities of the sanctioned tools, the enabling of more functionality for company tools or the complete blocking of these shadow IT tools. It could also result in the identification of tool gaps, where employees may require a specific functionality in order to effectively continue their work remotely.

Looking ahead
While for many implementing a collaboration tool may have been an urgent decision, it is likely that these new ways of working are here to stay. It is important, therefore, to set up your chosen tool for long-term success, thinking not only in terms of weeks or months, but years. What will happen to your data if you decide to change tools? How should employees handle data? What tools could we implement for improved efficiency?

To help you answer these questions, we as KPMG can leverage our knowledge, sector peers and industry good practices. In this way, you can keep your virtual collaboration safe in a pragmatic and efficient way.

Contact us

Koos Wolters
KPMG Cyber Partner
T: +31 (0)20 656 4048
E: wolters.koos@kpmg.nl

Edwin Sturrus
KPMG Cyber Manager
T: +31 (0)20 656 7248
E: sturrus.edwin@kpmg.nl