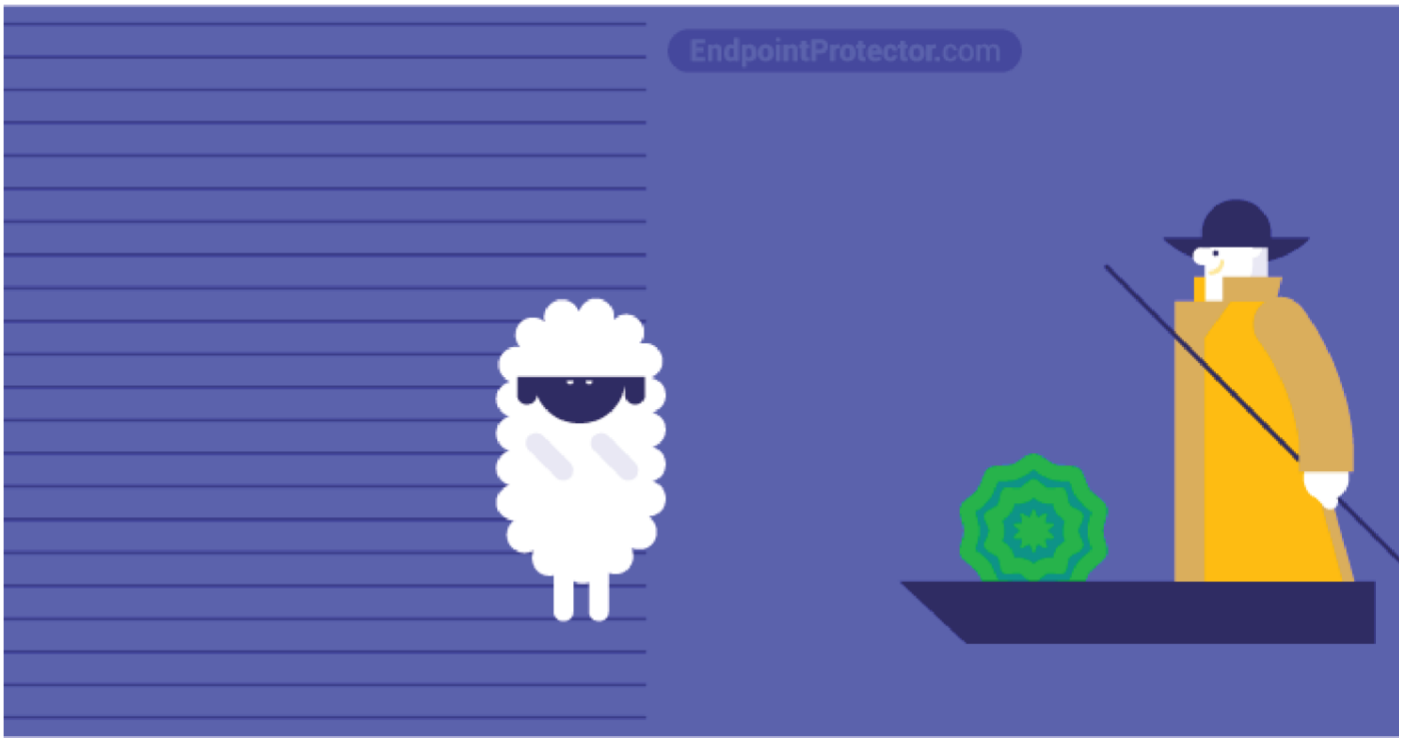

LES OUTILS COLLABORATIFS EN ENTREPRISE

Beata Berecki 8 août 2019.

Francisé par WaSaCa le Distributeur Référent de CoSoSys by Invintia en France, www.WaSaCa.fr

Avec l'adoption généralisée des plates-formes de collaboration (WSC « Worksteam Collaboration »), un nouvel équilibre entre la sécurité, la productivité et le mode collaboratif nomade est à définir dans toutes les entreprises.

La communication sur le lieu de travail continue d'évoluer. Le travail en équipe via des outils collaboratifs est en pleine croissance. Les plates-formes et applications WSC ont changés la façon dont les équipes interagissent. La prise en charge par ces outils de tous les flux d'informations modernes, accélère l'innovation, améliore la productivité et l'engagement de chacun. L'adoption d'une plate-forme de CSM, telle que Slack ou Mattermost, au sein des équipes permet un accès plus rapide aux informations pertinentes, intègre tous les flux de travail dans l'outil collaboratif. Ces plates-formes et applications rassemblent des fonctionnalités de chat, de partage de connaissances, d'appels, de robots, de recherche et de découverte et complètent le tout par des intégrations utiles. Elles sont également un facteur d'avantage concurrentiel et sont de plus en plus adoptées par les Entreprises.

Cependant, à l'ère des données sensibles, les plates-formes et applications WSC créent également un nouvel ensemble de vecteurs de menaces et introduisent des risques inhérents. Bien que la collaboration soit l'avenir du lieu de travail numérique, le partage en temps réel des données non structurées dans ces outils crée actuellement une lacune dans la sécurité globale de l'Entreprise. Les plates-formes et applications WSC sont relativement simples à adopter pour les utilisateurs, mais la surveillance et la sécurisation de l'environnement collaboratif est une tâche plus complexe.

Certaines applications ont des capacités de sécurité basique intégrées. Beaucoup d'Entreprises ne se rendent pas compte que la sécurité de leurs savoirs n'est peut-être pas suffisantes contre l'un des risques de sécurité les plus courants

- les fuites de données accidentelles ou intentionnelles.

Les flux de collaboration contiennent souvent des conversations et du contenu sensibles ; ainsi, la majorité des services de flux de travail utilisent le chiffrement. La confidentialité et la protection des données, qu'il s'agisse d'informations personnellement identifiables (IPI) ou de propriété intellectuelle (PI), est une préoccupation majeure pour les entreprises. En particulier à la lumière des réglementations de protection des données personnelles au niveau mondial telles que RGPD, CCPA, LGPD, etc...

Les données confidentielles doivent être protégées afin d'éviter les atteintes à la réputation, les amendes, les litiges et les pertes commerciales. L'envoi d'informations sensibles via des plates-formes collaboratives peut facilement les exposer, à l'intérieur ou à l'extérieur de l'Entreprise. La menace interne est très présente avec les outils de WSC comme Slack ou Matternost, que ce soit sous la forme d'un employé partageant accidentellement une base de données clients, d'une divulgation intentionnelle des business plans de l'entreprise ou d'un partage de numéros de sécurité sociale sur un cloud public.

Les politiques de sécurité et les procédures peuvent inclure des restrictions d'accès pour les « invités informatique », mais également une attention sécuritaire au suivi des applications utilisées, gestion du cycle de vie. D'autre part, les entreprises qui choisissent un outil collaboratif doivent être conscientes de l'efficacité de l'outil, de la facilité avec laquelle les utilisateurs peuvent partager les données conformément aux politiques de sécurité. La formation du personnel est une autre étape importante qui peut réduire davantage les risques de sécurité. Les Entreprises doivent s'assurer que leurs employés connaissent leurs politiques de sécurité et les pratiques appropriées en matière de partage des données auquel ils ont accès.

Les solutions de prévention des pertes de données (DLP) dotées de capacités de protection du contenu peuvent fournir aux entreprises utilisant des outils collaboratifs une couche de sécurité supplémentaire. Déployées, de telles solutions contrôlent les données confidentielles définis, peuvent facilement bloquer les données sur le point d'être partagées.

Certains logiciels DLP, comme Endpoint Protector, intègre déjà les définitions les plus courants de données protégées comme les IPI, les numéros de cartes de crédit, le code source et les expressions régulières. Ils offrent également la possibilité de protéger les données par type ou nom de fichier et bien sûr de définir un contenu personnalisé pour répondre à des besoins spécialisés.

Les solutions DLP peuvent également avoir des profils prédéfinis spéciaux pour différentes réglementations mondiale, RGPD, PCI DSS et HIPAA et accompagner les efforts des entreprises pour mettre en application la juridiction de ces réglementations. En même temps, en raison du nombre élevé de politiques prédéfinies pour les informations personnelles, les entreprises peuvent facilement créer des profils pour se conformer à leurs réglementations locales de protection des données. Ainsi, la gestion de la PI et des RPI, le respect des différentes réglementations devient plus facile et plus efficace.

La majorité des outils collaboratifs s'intègrent aux outils de stockage et de partage sur Cloud tels que Dropbox, Google Drive et Box. Il est important pour les entreprises de pouvoir filtrer les données téléchargées, sinon, des informations sensibles pourraient se retrouver dans le domaine public...

Les outils de collaboratifs sont de plus en plus adoptés pour leur efficience dans l'entreprise, mais sans contrôles et vérifications appropriés, ils exposent les entreprises à de sérieux risques.