***4 conseils de sÃ©curitÃ© des donnÃ©es au sein des workflows***
**Internet**
PostÃ© par : JulieM
PubliÃ©e le : 21/3/2022 13:00:00

Mettre en place un systÃ¨me de sÃ©curisation des donnÃ©es pour le traitement des documents est indispensable pour toutes les structures. En effet, toute organisation se doit de sÃ©curiser correctement ses donnÃ©es et ses documents.

Les petites et moyennes entreprises qui ne bÃ©nÃ©ficient pas des mÃªmes infrastructures informatiques que les plus grandes structures, ni de leur potentiel de protection, sont souvent les cibles de choix des hackers.

Toshiba TFIS, leader sur le marchÃ© de la gestion documentaire et de lâ□□impression, partage ses quatre principaux conseils pour garantir une sÃ©curisation efficace des donnÃ©es et des documents.

### *Conseil 1 : SÃ©curisation du processus dâ□□impression*

Chaque tÃ¢che dâ□□impression contient des informations qui ne doivent pas tomber entre de mauvaises mains. SÃ©curiser lâ□□imprimante nâ□□est pas la seule action Ã  mener. En effet, la sÃ©curisation se pose Ã  3 moments du processus dâ□□impression :

1. PremiÃ¨rement, la tÃ¢che dâ□□impression doit pouvoir Ãªtre envoyÃ©e en toute sÃ©curitÃ© via lâ□□utilisation dâ□□identifiants uniques, permettant dâ□□identifier lâ□□ordinateur et le profil de lâ□□utilisateur. Les logiciels dâ□□authentification unique (SSO) permettent ainsi dâ□□accÃ©der facilement et en toute sÃ©curitÃ© Ã  plusieurs applications et outils du rÃ©seau.

2. Le deuxiÃ¨me moment important dâ□□un point de vue sÃ©curitaire est lâ□□enregistrement provisoire des demandes dâ□□impression. Toute personne bÃ©nÃ©ficiant dâ□□un accÃ¨s sÃ©curisÃ©, enregistre ses impressions en cours, sans que celles-ci ne soient accessibles aux autres utilisateurs. Cette sÃ©curitÃ© Ã©vite lâ□□accÃ¨s dâ□□informations potentiellement confidentielles.

3. La troisiÃ¨me Ã©tape intervient lorsque lâ□□utilisateur libÃ¨re lâ□□impression. Pour ce faire, il est impÃ©ratif de lui demander de sâ□□identifier sur lâ□□imprimante de maniÃ¨re sÃ©curisÃ©e, afin de vÃ©rifier quâ□□il sâ□□agit du bon collaborateur. Un pass dâ□□accÃ¨s, par exemple, ou un code PIN personnel Ã  6 caractÃ¨res comprenant des chiffres, des lettres et des signes sont les solutions adÃ©quates.

### *Conseil 2 : Impression mobile*

Autant dans la sphÃ¨re privÃ©e que professionnelle, nous utilisons quotidiennement nos smartphones et nos tablettes. Lâ□□impression mobile reste une mÃ©thode simple et rapide pour les collaborateurs, mais pas moins risquÃ©e pour la sÃ©curitÃ© des organisations. Alors comment faire en sorte que ces appareils et ces donnÃ©es restent protÃ©gÃ©s ?

Dâ□□abord, il est important que lâ□□entreprise mette des appareils mobiles Ã  disposition de ses collaborateurs dont elle a la propriÃ©tÃ© et le contrÃ´le. Si ce nâ□□est pas envisageable, il faut alors sâ□□assurer que les employÃ©s nâ□□utilisent pas dâ□□appareils obsolÃ¨tes qui seraient susceptibles de laisser fuiter des donnÃ©es.

Il convient aussi de paramÃ©trer convenablement le processus dâ□□impression mobile Ã  lâ□□aide dâ□□un logiciel de gestion de lâ□□impression. Celui-ci protÃ©gera les tÃ¢ches dâ□□impression via lâ□□appareil mobile de la mÃªme faÃ§on que si elles Ã©taient effectuÃ©es depuis un ordinateur. Lâ□□utilisateur nâ□□aura alors quâ□□Ã  sâ□□identifier en toute sÃ©curitÃ© auprÃ¨s dâ□□une imprimante raccordÃ©e au logiciel, puis effectuer la tÃ¢che dâ□□impression dÃ©sirÃ©e.

### *Conseil 3 : NumÃ©risation et enregistrement*

Lorsquâ□□une entreprise numÃ©rise des documents, ces derniers restent enregistrÃ©s dans le cloud, dans un systÃ¨me de gestion des documents, voire dans le scanner. Il convient de protÃ©ger ces emplacements contre les cyberattaques potentielles en choisissant un partenaire fiable, de confiance et qui veillera constamment sur les donnÃ©es enregistrÃ©es.

Il est Ã©galement judicieux de verrouiller les documents et de les protÃ©ger par mot de passe. Ainsi, ils ne pourraient pas Ãªtre ouverts sâ□□ils tombaient entre de mauvaises mains.

ProtÃ©ger les documents nâ□□est pas seulement utile contre les cyberpirates, il existe aussi des risques liÃ©s Ã  lâ□□environnement interne, notamment lors dâ□□envois ou dâ□□impressions de documents. Pour rÃ©duire ce risque, il faut ajouter des Â« tampons de sÃ©curitÃ© Â» automatiques aux documents enregistrÃ©s dÃ¨s quâ□□ils sont imprimÃ©s, copiÃ©s ou envoyÃ©s par e-mail.

En intÃ©grant, par exemple, un nom dâ□□utilisateur, un dÃ©partement et lâ□□heure Ã  laquelle lâ□□action a eu lieu, il sera plus facile dâ□□identifier les utilisateurs internes et externes et ainsi de les dissuader de manipuler nÃ©gligemment des documents.

### Conseil 4 : SÃ©curisation des copies et traÃ§age

LÃ©galement, certains documents ne peuvent Ãªtre copiÃ©s ou numÃ©risÃ©s. Câ□□est notamment le cas des titres, tels que les billets de dollars ou dâ□□euros. Il est donc essentiel que les imprimantes reconnaissent de tels documents et les protÃ¨gent contre la copie, lâ□□impression et la numÃ©risation. La plupart des imprimantes multifonctions sont dÃ©jÃ  protÃ©gÃ©es contre ce genre de manipulation.

Il peut aussi Ãªtre souhaitable dâ□□empÃªcher la numÃ©risation ou lâ□□envoi de certains documents confidentiels. Pour ce faire, lâ□□entreprise peut mettre en place un logiciel de numÃ©risation Ã  reconnaissance de formulaire.

Cette solution permet dâ□□informer le logiciel sur les documents ne pouvant pas Ãªtre numÃ©risÃ©s ou envoyÃ©s. Naturellement, ce programme enregistrera et rapportera ces manipulations aux gestionnaires, Ã©vitant ainsi aux organisations dâ□□Ãªtre accusÃ©es de pratiques illÃ©gales.

Au fil de leurs dÃ©veloppements, les entreprises manipulent un nombre croissant de documents ; contrÃ´ler la sÃ©curitÃ© peut alors Ãªtre chronophage. Pour une sÃ©curisation complÃ¨te et un gain de temps optimal, il est recommandÃ© dâ□□adopter des conseils de sÃ©curitÃ© simples et efficaces pour lâ□□ensemble de ses workflows de traitement de documents.