CybersÃ©curitÃ© et sauvegarde : deux notions complÃ©mentaires
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 10/10/2023 13:00:00

Les sujets liÃ©s aux donnÃ©es et Ã la cybersÃ©curitÃ© sont devenus des Ã©lÃ©ments centraux Ã prendre en considÃ©ration dans les orientations stratÃ©giques de toutes les organisations.

Dans ce contexte, nombre dâ□□entreprises sont tentÃ©es de mettre sous le chapeau de la cybersÃ©curitÃ© de nombreuses notions, dont celle de la sauvegarde notamment.Â

Ces Ã©lÃ©ments sont complÃ©mentaires : la sauvegarde est un projet Ã part entiÃ¨re qui rÃ©pond Ã des mÃ©canismes particuliers et vient complÃ©ter la gouvernance cyber afin de sâ□□assurer que les donnÃ©es de lâ□□entreprise soient toujours disponibles.

La cybersÃ©curitÃ© : se protÃ©ger, se prÃ©munir ou se relever plus vite en cas dâ□□attaque

Lorsque lâ□□on parle de cybersÃ©curitÃ©, on fait rÃ©fÃ©rence Ã un ensemble de dispositifs qui ont pour unique objectif de protÃ©ger le systÃ¨me dâ□□information et les collaborateurs de lâ□□entreprise dâ□□attaques informatiques variÃ©es qui peuvent impacter ses opÃ©rations.Â

Protection des rÃ©seaux, des postes de travail, des Ã©changes, des attaques complexes de type Ddos, sensibilisation des collaborateurs, etc. sont autant dâ□□Ã©lÃ©ments constitutifs dâ□□une politique de dÃ©fense cyber.

On notera enfin que lâ□□un des principaux enjeux de la cybersÃ©curitÃ© est de sâ□□assurer que les donnÃ©es de lâ□□entreprise sont sÃ©curisÃ©es et quâ□□elles ne soient pas compromises et exfiltrÃ©es du SystÃ¨me dâ□□information.Â

Il sâ□□agit donc dâ□□avoir une dÃ©marche de protection et de surveillance pour parer aux tentatives dâ□□intrusion et de vol de donnÃ©es mais aussi aux erreurs humaines.

La sauvegarde : lâ□□assurance dâ□□accÃ©der Ã ses donnÃ©es Ã tout moment

Comme nous lâ□□avons Ã©voquÃ© prÃ©cÃ©demment, la cybersÃ©curitÃ© joue un rÃ´le central pour se protÃ©ger dâ□□attaques qui pourraient impacter les donnÃ©es de lâ□□ensemble de lâ□□entreprise. La sauvegarde rÃ©pond de son cÃ´tÃ© Ã un autre objectif.Â

Elle consiste en effet Ã mettre en Å□uvre un dispositif global qui permettra de sauvegarder automatiquement et, selon une frÃ©quence Ã dÃ©finir, lâ□□ensemble des donnÃ©es de lâ□□entreprise afin de prendre le relais en cas dâ□□Ã©chec des moyens de protection cybersÃ©curitÃ© mis en place.

Les donnÃ©es seront alors dupliquÃ©es et conservÃ©es dans des environnements de confiance et pourront au besoin Ãªtre restaurÃ©es en cas de paralysation du systÃ¨me dâ□□information. Lâ□□une des stratÃ©gies les plus efficaces reste la stratÃ©gie 3-2-1.

Elle consiste Ã sauvegarder 3 copies : deux copies sur 2 supports de stockages diffÃ©rents, afin de minimiser les risques potentiels de dÃ©faillance de lâ□□un dâ□□eux et, une derniÃ¨re copie hors site afin de contrer les actes de malveillance mais aussi se prÃ©munir de tout dommage liÃ© Ã un

sinistre (incendie, tempÃªte, court-circuitâ¦).Â

DÃ©ployer, paramÃ©trer et opÃ©rer de tels systÃ¨mes exige un trÃ¨s haut niveau dâexpertise, il est donc fondamental de se tourner vers des spÃ©cialistes en la matiÃ¨re.

A travers ces Ã©lÃ©ments, il apparait trÃ¨s clairement que les sujets liÃ©s Ã la sauvegarde sont Ã traiter avec la plus grande attention car ils viennent complÃ©ter les dispositifs de cybersÃ©curitÃ© dÃ©ployÃ©s par lâentreprise.

Au final, combiner solutions de cybersÃ©curitÃ© et mise en place dâune stratÃ©gie de sauvegarde industrielle est une rÃ©elle assurance de protÃ©ger et de pouvoir accÃ©der Ã ses donnÃ©es. Ainsi, lâentreprise peut poursuivre ses activitÃ©s sereinement et se concentrer sur son cÅur de mÃ©tier, dixit Laurent BENAMOU - DSI & RSSI chez Stordata