La sÃ©curitÃ© numÃ©rique, enjeu majeur de lâinnovation
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 19/1/2018 13:00:00

Les donnÃ©es sont devenues lâactif le plus prÃ©cieux des entreprises. Mais est-il le mieux gardÃ© ? Lâexposition des entreprises aux cybermenaces ne cesse de croÃ®tre avec la mobilitÃ© des collaborateurs, le partage des donnÃ©es, le dÃ©veloppement du Cloud computing, lâInternet des objets et lâintÃ©gration de nouvelles entitÃ©s.

La protection des informations numÃ©riques reprÃ©sente pour les entreprises un enjeu Ã©conomique fondamental et paradoxalement, assez souvent indÃ»ment nÃ©gligÃ©. Lâinnovation contemporaine est intimement liÃ©e aux donnÃ©es. A lâÃ¨re du digital elles constituent le nouvel actif stratÃ©gique des entreprises, dont la compÃ©titivitÃ© dÃ©pend aujourdâhui de leur capacitÃ© Ã contextualiser et analyser les masses accumulÃ©es de donnÃ©es.

Â

Chaque jour des milliers, voire des millions de nouveaux devices se connectent au grand Â« Internet of Everything Â» pour collecter et Ã©changer des donnÃ©es. Le marchÃ© se tourne vers des outils analytiques avancÃ©s pour les valoriser.Â

Ces nombreuses sources de collecte et dâaccÃ¨s aux donnÃ©es sont autant de points de fragilitÃ© pour les malfaiteurs voulant sâattaquer aux systÃ¨mes dâinformation et de production.

Si ces devices ne sont pas protÃ©gÃ©s, si sont compromises la disponibilitÃ©, la confidentialitÃ© et lâintÃ©gritÃ© des informations stockÃ©es, traitÃ©es ou transmises, lâavantage concurrentiel quâelles offrent risque de se transformer en pertes et la force devient une menace.

Le ROI en cybersÃ©curitÃ© : quâest-ce que vous Ãªtes prÃªts Ã perdre ?

Dans la sÃ©curitÃ© numÃ©rique, les cyberattaques sont le risque le plus connu. En France, onze incidents de cybersÃ©curitÃ© seraient comptabilisÃ©s chaque jour en milieu professionnel. Une rÃ©cente Ã©tude estime les pertes financiÃ¨res Ã 1,5 million d'euros pour chaque incident en moyenne.

Dans le monde, le nombre de cyberattaques aurait augmentÃ© en 2016 de 21% par rapport Ã lâannÃ©e prÃ©cÃ©dente, et cumulÃ©es, elles auraient coÃ»tÃ© Ã lâÃ©conomie mondiale 280 milliards de dollars, selon International Business Report (IBR) publiÃ© par le cabinet Grant Thornton. Mais le plus grand risque, et donc la plus grande crainte, ne se rÃ©sume pas aux pertes financiÃ¨res.

Par exemple, au Canada, 31,6 % des organisations sondÃ©es ont jugÃ© que la principale consÃ©quence dâune cyberattaque serait le temps passÃ© Ã traiter ses effets, suivi dâatteinte Ã la rÃ©putation (29,2 %) et perte de clients (10,2 %).Â

La perte directe de revenus nâa Ã©tÃ© citÃ©e que par 9,8 % dâinterrogÃ©s. MalgrÃ© cela, 52% des organisations nâont aucune couverture en cas dâattaque.

Selon moi, trop souvent encore les entreprises font appel aux experts Â« aprÃ¨s la bataille Â». Bien sÃ»r, nous sommes capables de gÃ©rer la crise, mais la prÃ©vention reste la meilleure rÃ©ponse aux cyberattaques.Â

Il est temps dâaccepter que le ROI de la cybersÃ©curitÃ© ne se calcule pas en chiffre dâaffaires gÃ©nÃ©rÃ©, mais plutÃ´t en efforts nÃ©cessaires Ã traiter les dommages potentiels. Il convient Ã toute entreprise, quâelle soit un grand groupe ou une PME, de mettre en place une vÃ©ritable stratÃ©gie de sÃ©curitÃ©, pour diminuer son exposition au risque et accompagner son dÃ©veloppement.

Pour une vÃ©ritable politique de sÃ©curitÃ© numÃ©rique

La premiÃ¨re Ã©tape consiste Ã faire appel Ã des experts pour Ã©valuer les facteurs de risque et les points faibles en matiÃ¨re de cybersÃ©curitÃ©. Ces Ã©lÃ©ments serviront Ã dÃ©finir une vÃ©ritable politique de sÃ©curitÃ© qui ne devra plus concerner la seule stratÃ©gie IT, mais Ãªtre intÃ©grÃ©e aux stratÃ©gies de tous les mÃ©tiers par une conduite de changement.

Effectivement, les facettes de la cybersÃ©curitÃ© sont dâautant plus nombreuses, que le sujet est transverse et concerne tous les mÃ©tiers de lâentreprise : la sÃ©curisation de lâÃ©cosystÃ¨me digital de lâentreprise et de ses outils collaboratifs, la gestion des identitÃ©s et des accÃ¨s, la prÃ©vention des pertes de donnÃ©es, etc.

Le cyberpiratage et les cyberattaques ne sont pas les seules menaces pour la sÃ©curitÃ© numÃ©rique, mais les plus mÃ©diatisÃ©es : dâexpÃ©rience, 35% des incidents de sÃ©curitÃ© seraient causÃ©s en interne par des collaborateurs mal informÃ©s.Â

Ainsi, la protection des informations va bien au-delÃ de la sÃ©curitÃ© : pour protÃ©ger tous les terminaux et points dâaccÃ¨s, il nâest plus question de se satisfaire dâun antivirus, aussi puissant soit-il.

Avant de se pencher sur des solutions technologiques, il est vital de comprendre son actuel niveau de maturitÃ©, dÃ©finir le niveau de sÃ©curitÃ© visÃ© et se faire accompagner pour instaurer une gouvernance, dÃ©finir des responsabilitÃ©s, revoir les rÃ¨gles et les procÃ©dures, et, finalement, envisager lâoutillage nÃ©cessaire.

Lâadoption de nouvelles technologies dâinformation continue dâaller beaucoup plus vite que la sÃ©curitÃ©. Au nom de la productivitÃ© et de la performance, les entreprises ont parfois

mis de cÃ´tÃ© les mesures de protection.Â

En se posant en bouclier protÃ©geant les donnÃ©es, les infrastructures et les nouvelles mÃ©thodes collaboratives de travail, la cybersÃ©curitÃ© sâaffirme en garant de lâinnovation et de la vitalitÃ© de lâentreprise.

David Adde, directeur du pÃ´le SÃ©curitÃ© chez Avanade