Les robots logiciels, nouvelle cible
Internet
PostÃ© par : JPilo
PubliÃ©e le : 24/1/2022 15:00:00

Ce 24 janvier 2022 marque le dÃ©but de la semaine europÃ©enne de la protection des donnÃ©es Ã caractÃ¨re personnel (Data privacy week). Cette annÃ©e, avec la montÃ©e en puissance des cybermenaces, lâ□□habituelle journÃ©e est devenue une semaine de sensibilisation. Cette derniÃ¨re a pour but de rappeler aux citoyens europÃ©ens lâ□□importance de la sÃ©curitÃ© de leurs donnÃ©es personnelles.

A ce sujet, David Higgins, Directeur technique chez CyberArk, rappelle que cette protection nâ□□est pas uniquement imputable aux humains mais doit Ãªtre Ã©galement Ã©tendue aux robots logiciels :

Â« Les humains ne sont pas les seuls susceptibles de cliquer sur le mauvais lien ou de partager trop dâ□□informations sur eux-mÃªmes. Les robots logiciels ont Ã©galement des problÃ¨mes de partage, et en cette Data Privacy Week, il est important de comprendre comment mieux protÃ©ger les donnÃ©es auxquelles ils accÃ¨dent.

Les robots logiciels â□□ constituÃ©s de petits morceaux de code qui effectuent des tÃ¢ches rÃ©pÃ©titives â□□ sont dÃ©sormais nombreux dans les entreprises du monde entier, ainsi que dans les banques, les instances gouvernementales et tous les autres grands secteurs verticaux.

Ils ont pour objectif de libÃ©rer du temps au personnel, afin que les employÃ©s puissent travailler sur des tÃ¢ches davantage critiques, cognitives et crÃ©atives. Mais les robots logiciels contribuent Ã©galement Ã amÃ©liorer l'efficacitÃ©, la prÃ©cision, l'agilitÃ© et l'Ã©volutivitÃ©. De ce fait, ils sont une composante majeure de l'entreprise numÃ©rique.

Or, ces robots ont parfois recours Ã des donnÃ©es sensibles pour mener Ã bien leurs missions, ce qui peut poser un problÃ¨me de confidentialitÃ©. Par exemple, ils peuvent devoir rassembler des donnÃ©es mÃ©dicales sensibles et personnelles pour aider les mÃ©decins Ã faire des prÃ©dictions cliniques Ã©clairÃ©es. Aussi, ils auraient besoin dâ□□un accÃ¨s pour traiter des donnÃ©es clients stockÃ©es sur un serveur cloud public ou un portail web.

Ces derniÃ¨res annÃ©es regorgent dâ□□exemples de problÃ¨mes liÃ©s Ã la compromission dâ□□utilisateurs, une situation similaire que lâ□□on retrouve avec les robots et Ã plus grande Ã©chelle. Si ces derniers sont mal configurÃ©s et codÃ©s, et quâ□□ils peuvent accÃ©der Ã plus de donnÃ©es qu'ils n'en ont besoin, in fine, ces donnÃ©es peuvent en effet Ãªtre divulguÃ©es et se retrouver lÃ oÃ¹ elles ne devraient pas Ãªtre.

De mÃªme, la menace interne est de plus en plus prÃ©sente et des identitÃ©s humaines sont compromises presque quotidiennement pour accÃ©der Ã des donnÃ©es sensibles. Les machines ont exactement les mÃªmes problÃ¨mes de sÃ©curitÃ© ; si elles peuvent accÃ©der Ã des informations critiques sans Ãªtre correctement sÃ©curisÃ©es, elles reprÃ©sentent une porte ouverte pour les hackers.

Une porte qui peut mettre en danger la vie privÃ©e des individus. Les cybercriminels ne ciblent pas que les utilisateurs pour accÃ©der aux donnÃ©es, ils ciblent directement les informations quâ□□ils recherchent. Si les machines, en particulier celles en charge des processus automatisÃ©s, sont le

meilleur chemin Ã emprunter pour y accÃ©der, c'est celui que les pirates informatiques choisiront. Â»