CybersÃ©curitÃ© : Les trois prÃ©dictions de Venafi pour 2019

Internet

PostÃ© par : JulieM
PubliÃ©e le : 13/12/2018 13:00:00

Les violations de donnÃ©es deviendront encore plus dÃ©vastatrices Ã mesure que lâangle d'attaque de l'identitÃ© des machines s'Ã©largira.
Malheureusement, les entreprises nÃ©gligent cet angle dâattaque croissant, et potentiellement dÃ©vastateur : les machines.

Selon Business Insider, plus de 24 milliards dâappareils connectÃ©s Ã Internet seront installÃ©s d'ici 2020 ; plus de quatre appareils pour chaque personne sur la planÃ¨te. Ces dispositifs, avec leurs algorithmes, les conteneurs et bien plus encore, ont leur propre identitÃ©.

Les organisations dÃ©pensent plus de huit milliards de dollars pour protÃ©ger les identitÃ©s humaines, mais quasiment rien pour protÃ©ger les identitÃ©s des machines. Les cyberpirates le savent et consacrent dÃ©sormais plus de temps et de ressources pour cibler les identitÃ©s faibles, vulnÃ©rables ou compromises des machines.

Les vilains continueront Ã gagner du terrain dans les annÃ©es Ã venir, Ã fortiori si les identitÃ©s des machines demeurent sans protection.

L'augmentation des usurpations d'identitÃ© Ã©largira le fossÃ© de la pauvretÃ© en matiÃ¨re de cyber-compÃ©tences. Les entreprises prÃ©voient dÃ©jÃ une pÃ©nurie mondiale dâ 1,8 millions dâemployÃ©s en matiÃ¨re de cybersÃ©curitÃ© dâici 2022.

La pÃ©nurie croissante de professionnels de la cybersÃ©curitÃ© va crÃ©er un Ã©cart de pauvretÃ© entre les organisations qui peuvent se permettre les bonnes compÃ©tences, et celles qui ne le peuvent pas.

Les entreprises sans personnel suffisamment qualifiÃ© commenceront Ã tomber sous le Â« seuil de pauvretÃ© Â» de la cybersÃ©curitÃ©, et seront ciblÃ©es et violÃ©es plus frÃ©quemment par les cybercriminels. En fin de compte, cela concerne tout le monde, mÃªme les entreprises Ã sÃ©curitÃ© renforcÃ©e, car leur "maillon le plus faible" pourrait Ãªtre lâ□□un de leurs partenaires.

Malheureusement, le fossÃ© en matiÃ¨re de cyber-compÃ©tences se creuse Ã mesure que lâ□□angle dâ□□attaque dans le monde sâ□□Ã©largit. La transformation numÃ©rique en cours dÃ©pend entiÃ¨rement des machines, pas des personnes, et dans la plupart des cas, ces machines ne sont pas protÃ©gÃ©es.

Le vol dâ□□identitÃ© verra un Â« tournant Â».

En 2018, plus dâ□□un tiers des consommateurs du monde ont Ã©tÃ© victimes de fraude par carte de crÃ©dit ou de dÃ©bit. Cela peut avoir un impact grave sur les Ã©valuations de crÃ©dit, car les entreprises sont contraints de faire un choix difficile : exclure les clients qui semblent risquÃ©s - potentiellement sans responsabilitÃ© de leur part - ou assouplir leurs critÃ¨res dâ□□Ã©valuation et sâ□□ouvrir Ã un risque supplÃ©mentaire.

Les Ã□tats-Unis ont dÃ©jÃ constatÃ© l'impact de cette situation, ayant introduit un gel des crÃ©dits Ã la consommation sans frais en 2018 dans le cadre du dÃ©mantÃ¨lement de la loi Dodd-Frankt. Malheureusement, la plupart des organisations se concentrent sur l'impact du vol d'identitÃ© humaine, tout en ignorant les consÃ©quences d'une protection faible d'identitÃ© des machines.

Selon Justin Hansen :

Â« Globalement, 2019 sera une annÃ©e difficile pour les Ã©quipes de sÃ©curitÃ©. Il est probable que les tendances en matiÃ¨re de violations observÃ©es en 2018 se poursuivront, et les consÃ©quences seront sÃ©rieuses tant pour les entreprises que pour les consommateurs.

En fin de compte, l'explosion du nombre de machines connectÃ©es Ã Internet - des services Cloud aux applications mobiles et Ã l'IdO - crÃ©e un terrain de jeu pour les cyberespaces qui souhaitent infiltrer et voler des donnÃ©es.

Tant que les entreprises ne pourront contrÃ´ler et protÃ©ger les identitÃ©s de leurs machines, des incidents majeurs de sÃ©curitÃ© continueront Ã se dÃ©velopper, tant au niveau de leur amplitude que de leurs impacts Â».

Justin Hansen, security architect pour le leader de la protection d'identitÃ© des machines Venafi