L'informatique quantique ne doit pas nous inquiÃ©ter (pour le moment)
Internet
PostÃ© par : JulieM
PubliÃ©e le : 17/3/2023 13:00:00

Dans le jeu du chat et de la souris de la cybersÃ©curitÃ©, il est essentiel dâessayer dâanticiper la prochaine technologie de rupture. Quelle sera la prochaine avancÃ©e, et comment Ã©viter de se laisser distancer ? Parmi les candidats figure lâinformatique quantique. Mais au-delÃ de son Ã©norme potentiel, cette technologie prÃ©sente Ã©galement des dÃ©fis de taille, en particulier dans le domaine de la cybersÃ©curitÃ©.

Le 21 dÃ©cembre 2022, le PrÃ©sident des Ãtats-Unis Joe Biden a promulguÃ© le Quantum Computing Cybersecurity Preparedness Act. Cette loi promeut la prÃ©paration aux risques cyber liÃ©s Ã lâutilisation de lâinformatique quantique et encourage les organismes fÃ©dÃ©raux Ã adopter des technologies rÃ©sistantes aux tentatives de dÃ©cryptage Ã lâaide de cette technologie.

Cette manÅuvre peut donner lâimpression que les cyberattaques exploitant la puissance de lâinformatique quantique sont imminentes, et est susceptible de provoquer de la nervositÃ© au sein des secteurs publics comme privÃ©s.Â

Pourtant, lâheure nâest pas encore Ã la panique. IntÃ©ressons-nous Ã ces dangers, et dÃ©couvrons pourquoi la plupart des individus, en particulier dans le secteur privÃ©, nâont pas Ã sâen inquiÃ©ter dans un avenir immÃ©diat.

Les risques cyber liÃ©s Ã lâinformatique quantique

La principale crainte au sujet de lâinformatique quantique concerne son utilisation pour dÃ©crypter des donnÃ©es. Ã lâheure actuelle, le modÃ¨le de sÃ©curitÃ© de lâinformation repose sur cinq piliers : la confidentialitÃ©, lâintÃ©gritÃ©, la disponibilitÃ©, lâauthentification et la non-rÃ©pudiation.

Tous ces principes sâappuient (au moins en partie) sur le chiffrement Ã clÃ© publique, qui profite de la complexitÃ© de la dÃ©composition de nombres premiers pour des ordinateurs.

L'informatique quantique va cependant briser cette barriÃ¨re, ce qui va mettre en danger non seulement les informations nouvellement volÃ©es, mais aussi toutes les informations qui ont Ã©tÃ© prÃ©cÃ©demment interceptÃ©es et stockÃ©es par les pirates.

La vulnÃ©rabilitÃ© du chiffrement Ã clÃ© publique met donc lâessentiel de notre Ã©conomie numÃ©rique en danger, et nÃ©cessite lâadoption dâune toute nouvelle approche â Ã savoir la migration vers des algorithmes plus rÃ©sistants Ã cette puissance de calcul.

Et bien que de tels algorithmes existent dÃ©jÃ , nous ne pouvons garantir leur efficacitÃ©, car il nâexiste pas dâordinateur quantique suffisamment puissant pour les valider. En outre, lâutilisation de tels algorithmes impliquera un long (et pÃ©nible) processus dâimplÃ©mentation Ã travers lâensemble de lâenvironnement.

Pourquoi la plupart des organisations nâont pas Ã sâinquiÃ©ter (pour le moment)

Bonne nouvelle : selon les prÃ©visions les plus rÃ©alistes, il nous faudra attendre encore au moins

une dÃ©cennie pour voir apparaÃ®tre un ordinateur quantique capable de dÃ©composer des nombres premiers avec un taux dâerreur suffisamment faible pour Ãªtre utilisable.

En outre, les entreprises et gouvernements occidentaux bÃ©nÃ©ficient actuellement des capacitÃ©s de recherche les plus avancÃ©es dans ce domaine. Par consÃ©quent, si la tendance actuelle se confirme, beaucoup dâentreprises et la plupart des organismes fÃ©dÃ©raux auront le temps de se prÃ©parer avant que cette menace se concrÃ©tise.

Ceci Ã©tant dit, cette Ã©chÃ©ance lointaine nâoffre quâun modeste rÃ©confort aux organisations ayant dÃ©jÃ Ã©tÃ© victimes de fuites de donnÃ©es Ã longue durÃ©e de vie.

Bien quâil reste du temps pour mettre en Åuvre de nouvelles approches de sÃ©curitÃ© afin de mieux nous protÃ©ger des cyberattaques quantiques, en revanche, les donnÃ©es que les acteurs malveillants ont dÃ©jÃ entre leurs mains risquent de ne pas rÃ©sister bien longtemps.

Si la plupart des organisations nâont pas de donnÃ©es risquant dâÃªtre encore critiques dans une dizaine dâannÃ©es, câest en revanche le cas de celles qui traitent des informations relevant, par exemple, de la sÃ©curitÃ© intÃ©rieure.

Que faire dÃ¨s maintenant ?

En rÃ©alitÃ©, il nây a pas grand-chose que les organisations puissent faire Ã cet instant. Ã lâheure actuelle, tout tourne autour de la planification.Â

Des stratÃ©gies doivent Ãªtre dÃ©veloppÃ©es pour assurer une migration Ã grande Ã©chelle vers des algorithmes rÃ©sistants au calcul quantique, et pour dÃ©couvrir comment gÃ©rer les consÃ©quences du dÃ©cryptage de donnÃ©es sensibles ayant fait lâobjet de fuites par le passÃ©.

Le risque le plus important Ã ce jour est justement le fait que les organisations sâinquiÃ¨tent trop de la faÃ§on de gÃ©rer la menace potentielle que reprÃ©sente lâinformatique quantique, au lieu de concentrer leur Ã©nergie sur les questions plus concrÃ¨tes de leur cyberhygiÃ¨ne.Â

Les e-mails de phishing constituent actuellement une menace encore plus grande. Sâil est important de tenir compte des menaces de demain, notre prioritÃ© doit rester celles dâaujourdâhui.

Dans une dÃ©cennie, lâinformatique quantique pourrait bien remettre en cause les fondements de la sÃ©curitÃ© de lâinformation, et devenir par consÃ©quent une prÃ©occupation majeure.

Aucune information ne saurait Ãªtre considÃ©rÃ©e comme confidentielle, authentique, accessible (aux parties adÃ©quates) ou traÃ§able si les technologies sous-jacentes peuvent Ãªtre contournÃ©es. Mais aujourdâhui, il nous reste encore plus que suffisamment de temps pour nous prÃ©parer.

En attendant, nous avons davantage Ã gagner Ã mettre en place de bonnes politiques de cyber-hygiÃ¨ne pour nos environnements actuels, et Ã prÃ©parer nos organisations Ã faire preuve dâagilitÃ©.

Dans le domaine de la cybersÃ©curitÃ©, une dÃ©cennie reprÃ©sente beaucoup de temps. Il est donc improbable que lâinformatique quantique reste la seule technologie Ã bousculer lâordre Ã©tabli, dixit Rob Jenks, Vice-prÃ©sident sÃ©nior de la stratÃ©gie chez Tanium.