Livre blanc

Planifier la cybersécurité post-quantique

Il est temps de protéger les organisations et les données contre la menace que représente l'informatique quantique

KEYFACTOR

Table des matières

La dualité de l'informatique quantique 3

Planifier des solutions à court et à long terme pour faire face au piratage quantique..... 5

Les mesures à prendre pour aller de l'avant..... 7

01 S'engager dans la planification stratégique..... 7

02 Adopter une approche saine en matière d'inventaire et de sécurité des données et des appareils..... 8

Planter votre arbre de protection contre les menaces informatiques quantiques il y a 20 ans ou maintenant 9

Conclusion..... 9

Les promesses de l'informatique quantique sont alléchantes. Des tâches qui prendraient plusieurs centaines ou milliers d'années avec des ordinateurs binaires classiques pourraient être accomplies en quelques jours, voire quelques heures, avec des machines quantiques suffisamment puissantes.

Selon un rapport de Deloitte de 2021, la quasi-totalité des industries et des organismes gouvernementaux bénéficiera de l'augmentation exponentielle de la puissance de calcul permise par l'informatique quantique. Que ce soit l'optimisation de la chaîne d'approvisionnement, l'analyse des risques financiers, la simulation du changement climatique ou la découverte de nouveaux matériaux semi-conducteurs, les technologies quantiques promettent une révolution aussi importante que l'avènement de l'ordinateur personnel.

Mais un vieux dicton dit que toute solution contient les graines du prochain problème. Ce dicton est également valable dans le monde de l'après-quantique. Tous les outils de chiffrement et d'identification utilisés aujourd'hui pour protéger les données et l'identité seront rendus virtuellement inutiles et deviendront des proies faciles pour les pirates quantiques.

Mais cela n'est pas une fatalité. Si les gouvernements, les industries et les organisations commencent dès maintenant à planifier un environnement post-quantique, nous pourrons encore profiter des avantages de l'informatique quantique tout en atténuant les menaces pour la cybersécurité.

La dualité de l'informatique quantique

En mai 2022, la Maison-Blanche a publié un décret visant à renforcer la poursuite par le gouvernement fédéral d'un leadership international dans le domaine de l'informatique quantique. Le même jour, elle a également publié un mémorandum de sécurité nationale ordonnant aux agences fédérales de prendre des mesures pour atténuer les risques de l'informatique quantique.

Ce mémo sur la sécurité nationale souligne clairement les risques. Il indique, notamment :

> **"En particulier, un ordinateur quantique d'une taille et d'une sophistication suffisantes (également connu sous le nom d'ordinateur quantique pertinent du point de vue cryptanalytique, ou CRQC) sera capable de casser une grande partie des systèmes de chiffrement à clé publique employés dans les systèmes numériques aux États-Unis et dans le reste du monde. Quand il deviendra disponible, un CRQC pourrait compromettre les communications civiles et militaires, saper les systèmes de surveillance et de contrôle des infrastructures critiques et mettre en échec les protocoles de sécurité de la plupart des transactions financières sur Internet.**

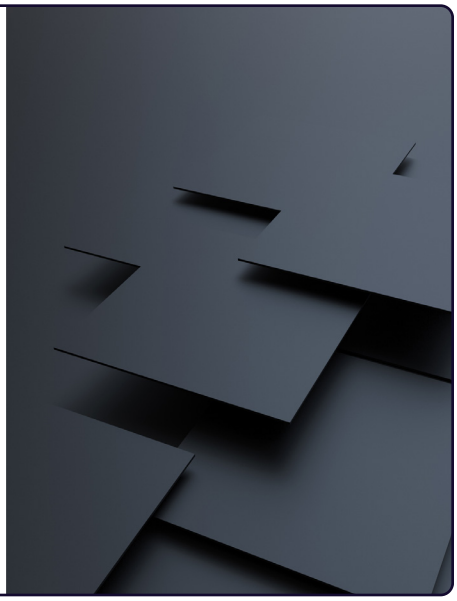
Imaginez : d'un côté, le gouvernement se consacre au développement de l'informatique quantique et à la définition de ses normes ; de l'autre, il avertit les agences qu'elles doivent prendre des mesures dès maintenant pour s'en protéger, même si elle n'existe pas encore.

Cette apparente contradiction s'explique par le fait que l'immense potentiel de l'informatique quantique, qui permet de résoudre des problèmes auparavant trop importants, peut également être utilisé pour pirater un élément essentiel de l'environnement informatique actuel : le chiffrement.

Par exemple, le schéma de chiffrement RSA de l'infrastructure à clé publique (ICP) est basé sur la multiplication de très grands nombres premiers ; utiliser un des ordinateurs actuels pour le résoudre prendrait environ 300 billions d'années, ce qui le rend pour ainsi dire insoluble. Mais un ordinateur quantique suffisamment puissant pourrait casser le même code de chiffrement en quelques minutes, ou potentiellement plus rapidement encore.

C'est pourquoi les agences fédérales déploient tant d'efforts pour empêcher l'exfiltration des données, même si elles s'attachent à exiger le chiffrement des données au repos et en transit.

Il existe un piratage « pré-quantique », qui consiste à voler des données pour les déchiffrer plus tard. Les pirates, souvent des États-nations hostiles, savent que les informations chiffrées qu'ils volent aujourd'hui pourront un jour être déchiffrées par la technologie quantique ; ils pourront alors déterminer quelle partie de leurs données volées est la plus utile. Ainsi, les attaques actuelles d'exfiltration de données pourraient devenir les atteintes à la sécurité nationale de demain, une fois qu'un ordinateur quantique sera capable de casser le chiffrement des données volées.



L'augmentation de la puissance des ordinateurs quantiques pourrait également avoir pour conséquence l'impossibilité pour tout utilisateur de naviguer sur Internet en toute sécurité. La petite icône en forme de cadenas à côté de l'URL signifie qu'elle utilise le protocole TLS (Transport Layer Security), qui a été développé par l'Internet Engineering Task Force (IETF), un organisme international de normalisation. La première version du protocole a été publiée en 1999, et sa dernière mise à jour remonte à 2018. Cependant, ce protocole a été conçu pour assurer une protection contre les menaces actuelles, et non contre celles posées par les machines quantiques.

Le protocole TLS est conçu pour assurer la confidentialité et la sécurité des données pour les communications sur Internet. Le piratage quantique réduirait son utilité à néant. L'IETF étudie déjà les moyens de maintenir la sécurité du protocole TLS dans un environnement post-quantique, mais en définitive, la seule façon de savoir si les nouvelles protections fonctionnent est de les utiliser sur le terrain, ce qui représente un pari risqué.

L'utilisation d'un ordinateur quantique comme outil de piratage s'apparente à une attaque par force brute, mais la comparaison s'arrête là. Le directeur technique d'une société travaillant sur des solutions post-quantiques, lui-même un expert en chiffrement, a déclaré qu'il existe des moyens de programmer un ordinateur quantique cryptographiquement pertinent (CRQC) de manière à ce qu'il utilise non

pas la force brute, mais les particularités de l'informatique quantique elle-même. « Il suffit de créer une simulation du nombre [à pirater], de définir les règles que le CRQC doit suivre, d'inculquer ces propriétés aux mille ou deux mille qubits, puis d'appuyer sur un bouton et de lancer le processus », a-t-il déclaré. « Le système quantique se stabilisera dans l'état qui résout le problème en un temps dérisoire. Vous trouverez peut-être quelques centaines de solutions plausibles, mais il est alors facile d'utiliser ensuite un ordinateur conventionnel pour déterminer laquelle de ces solutions est la bonne. »

Cet exemple n'est que le premier qui démontre l'étrangeté du fonctionnement de l'informatique quantique. Dans cet exemple, le verbe « stabiliser » fait penser à une boule sur une roulette qui rebondirait jusqu'à ce qu'elle se stabilise dans une seule et unique case. Dans le cas de l'informatique quantique, tous les qubits rebondissent et se stabilisent dans un état 1 ou 0, créant ainsi des centaines de solutions possibles. En outre, les ordinateurs quantiques, s'ils sont programmés correctement, peuvent y parvenir sans recourir aux tactiques traditionnelles de force brute utilisées par les ordinateurs binaires. En d'autres termes, il peut atteindre son objectif sans avoir à essayer toutes les combinaisons de nombres ou de solutions possibles au passage.

Planifier des solutions à court et à long terme pour faire face au piratage quantique

Il est clair que traiter les risques inhérents à la technologie de l'informatique quantique est essentiel pour la sécurité et le bien-être économique des nations.

Solutions pour la sécurité nationale

Le mémorandum de la Maison-Blanche sur la sécurité nationale répartit les responsabilités pour trouver des solutions à long terme. Plus précisément, il établit que :

> **" Actuellement, le directeur du National Institute of Standards and Technology (NIST) et le directeur de la National Security Agency (NSA), agissant en tant que directeur national des systèmes de sécurité nationale (directeur national), élaborent chacun des normes techniques de chiffrement résistant à l'informatique quantique pour leurs juridictions respectives.**

Pour se conformer à ce mémo, le NIST a sélectionné quatre algorithmes de chiffrement « résistants à l'informatique quantique » (RQ) et a commencé à les tester en juillet 2022. À la mi-août, l'un d'entre eux avait déjà été cassé en seulement quatre minutes, par un ordinateur de bureau ordinaire vieux de 10 ans.

En septembre, la NSA a publié son propre document d'information approuvant les choix d'algorithmes initiaux du NIST, afin de « définir les exigences futures [des systèmes de sécurité nationale], de façon à ce que les fournisseurs puissent commencer à s'y conformer et que les responsables des acquisitions, ainsi que les propriétaires et les exploitants des systèmes de sécurité nationale en prennent connaissance ». Le document indique que la transition vers les algorithmes RQ devrait être achevée d'ici 2035. En d'autres termes, les entreprises au service de la communauté du renseignement devraient commencer à intégrer immédiatement l'un des futurs algorithmes de chiffrement RQ du NIST.

Il s'agit d'un pari risqué, comme en atteste l'échec quasi immédiat de l'un des algorithmes testés ; mais dans le monde de la sécurité nationale, le jeu en vaut la chandelle. Il s'agit d'une combinaison de tactiques à court terme et de stratégie à long terme : dans un premier temps, il s'agit d'utiliser l'un de ces algorithmes afin que, lorsque le piratage quantique deviendra une réalité, les systèmes soient déjà prêts à s'en protéger.

Solutions de sécurité économique

Le défi pour les agences et les entreprises qui ne font pas partie de la communauté du renseignement et qui dépendent encore des communications chiffrées est de savoir comment se préparer à cet avenir périlleux, sans nécessairement parier sur l'un des algorithmes du NIST avant que son efficacité n'ait été prouvée.

Pour les organisations, l'informatique quantique nécessitera des efforts considérables pour garantir leur sécurité. Le problème, c'est que nombre d'entre elles ne savent pas où le chiffrement est utilisé et pour quelles données. Dans un monde idéal, nous disposerions d'un gros bouton rouge sur lequel serait inscrit « ne pas appuyer avant le jour de l'informatique quantique ou avant que le protocole RSA ne soit obsolète ». C'est ce que souhaitent les organisations, mais aucun moyen simple n'existe pour y parvenir.

Les mesures à prendre pour aller de l'avant

Si les organisations attendent l'invention d'un ordinateur quantique capable de casser les systèmes de chiffrement, il sera alors beaucoup trop tard pour commencer à s'en protéger. Pour éviter cette situation, plusieurs mesures clés doivent être prises dès maintenant pour faire en sorte que la sécurité informatique de votre agence, entreprise ou organisation parte du bon pied après l'arrivée de l'informatique quantique.

Étape 01

S'engager dans la planification stratégique

Toute organisation utilisant un système de chiffrement à l'heure actuelle doit se préparer à un avenir post-quantique. Mais le problème ne s'arrête pas là. Tout secteur qui fabrique des produits dont la durée de vie est supérieure à cinq ans, comme le secteur automobile, les appareils médicaux, les appareils ménagers et tout ce qui relève de l'Internet des objets (IoT), sera touché.

Par exemple, le secteur financier se prépare déjà à cet avenir. Wells Fargo a créé une division entièrement consacrée à la préparation de l'informatique post-quantique, et d'autres banques lui emboîtent le pas. Cependant, dans de nombreux autres domaines, on ne sait pas encore ce qu'implique l'informatique post-quantique, malgré le danger que représenterait un manque de préparation.

En d'autres termes, les organisations doivent se défaire de leur vision à court terme, centrée sur les résultats attendus pour le trimestre suivant, et adopter une vision à plus long terme de la sécurité pour se préparer à l'environnement de l'informatique post-quantique.

On peut comparer cela à la façon dont les organisations doivent se préparer à une catastrophe naturelle (ou d'origine humaine), non pas parce que celle-ci est imminente, mais parce que si elle est imminente, il est trop tard pour s'y préparer. Les organisations doivent faire le nécessaire et perfectionner leurs normes de cybersécurité. Par exemple, si elles modernisent leur infrastructure pour mettre en œuvre une architecture de type « confiance zéro », elles doivent investir dans des produits qui intègrent des mesures de préparation à un environnement informatique post-quantique.

Étape 02

Adopter une approche saine en matière d'inventaire et de sécurité des données et des appareils

De nombreuses organisations, notamment dans le secteur privé, ne connaissent pas parfaitement tous les appareils connectés à leurs systèmes, ni les mesures de sécurité qu'elles utilisent, ni les emplacements où le chiffrement est utilisé dans leurs immenses réseaux. Elles ne sont pas non plus en mesure de déterminer quelles données sont les plus vulnérables et quelles données sont les plus précieuses.

Il est intéressant de noter que les organismes fédéraux sont mieux placés pour identifier et suivre leur utilisation du chiffrement en raison du cadre réglementaire dans lequel ils opèrent. Cela s'explique par le fait que le gouvernement adopte une approche écosystémique. Des éléments comme le BYOD, le travail à domicile et l'authentification multifacteur, par exemple, sont des domaines dans lesquels les agences sont susceptibles d'avoir un meilleur contrôle. Ce n'est que depuis peu que l'industrie commence à se pencher sérieusement sur la question.

Ainsi, la première véritable étape informatique, après avoir obtenu le soutien de la haute direction en faveur d'une préparation à long terme, consiste à développer cet inventaire et à s'engager à le tenir à jour.

Cela s'applique également aux industries utilisant la technologie de l'IoT. Les entreprises qui conçoivent et fabriquent des appareils IoT, qu'ils soient médicaux, résidentiels ou commerciaux, doivent intégrer des capacités mises à jour et intégrer la gestion du cycle de vie de la composante cryptographique dans ces appareils.

Pour les organisations qui adoptent une architecture de type « confiance zéro », que ce soit dans le secteur public ou privé, la transition elle-même est l'occasion d'identifier les domaines dans lesquels le chiffrement est utilisé et les appareils qui sont connectés. Cela permet de limiter les interventions réactives. Vous aurez déjà des inventaires et des priorités entièrement définis.

Cela permet également de tirer parti de l'automatisation, par exemple en remplaçant les certificats de type « confiance zéro » par des certificats prenant en charge des algorithmes résistants à l'informatique quantique, et ce dans plusieurs emplacements à la fois.

Il s'agit d'une étape importante, car la pénurie de main-d'œuvre dans le domaine de la cybersécurité constitue déjà un goulot d'étranglement majeur, en particulier lorsqu'il s'agit de trouver des personnes possédant des compétences spécialisées dans des domaines tels que le chiffrement et les ICP. La capacité d'automatiser les tâches permettra de maintenir les stocks à jour et de se convertir rapidement à l'environnement post-quantique.

Planter votre arbre de protection contre les menaces informatiques quantiques il y a 20 ans ou maintenant

Le meilleur moment pour planter un arbre était il y a 20 ans, dit le vieux dicton. Et le deuxième meilleur moment pour en planter un est aujourd'hui. Ce dicton est pertinent, car il faut de nombreuses années à un arbre pour atteindre le stade où l'homme est en mesure de profiter de ses bienfaits : des noix ou d'autres fruits, de l'ombre en été, des avantages environnementaux, voire du bois d'œuvre. Le deuxième meilleur moment pour planter un arbre est aujourd'hui, car attendre ne fera que retarder le moment où ses bienfaits pourront commencer à s'accumuler.

Il en va de même pour l'investissement dans une sécurité informatique résiliente. Cela ne peut pas se faire du jour au lendemain, et lorsque vous en aurez vraiment besoin, il sera trop tard pour régler le problème. Si vous voulez être prêt pour l'avenir post-quantique, vous devez préparer le terrain dès maintenant.

Le bug de l'an 2000, un problème qui aurait pu frapper les ordinateurs à la fin du XXe siècle, est un bon exemple de résolution précoce d'un problème. En effet, il a été constaté que les ordinateurs ne disposant pas de champs de date suffisamment étendus risquaient de tomber en panne lorsque l'horloge sonnerait minuit en l'an 2000, car leurs systèmes d'exploitation et leurs applications penseraient qu'il s'agit de l'année 1900, voire de l'année zéro. Heureusement, le problème a été découvert des années avant la date critique. La catastrophe du passage à l'an 2000 ne s'est jamais produite, parce que nous avons pris le problème au sérieux. La sécurité informatique post-quantique doit faire l'objet du même niveau d'attention, car si elle n'est pas traitée rapidement, les conséquences seront très graves.

Conclusion

L'informatique quantique ouvre un monde de possibilités entièrement nouveau, et il ne fait aucun doute qu'elle contribuera à faire progresser notre société dans des proportions sans précédent.

Cependant, elle bouleversera aussi fondamentalement les algorithmes utilisés pour l'ICP. En fin de compte, la question de savoir si l'informatique quantique atteindra ou non la taille et l'échelle nécessaires pour casser efficacement les algorithmes existants est sans objet. Dans les faits, les organisations devront adopter de nouveaux algorithmes, car la menace existe et existera toujours. Une fois que le nouvel ensemble d'algorithmes résistants à l'informatique quantique sera approuvé et normalisé, il ne sera plus possible de revenir en arrière. Les nouveaux risques auxquels nous serons confrontés sont importants, mais ils sont également gérables si nous commençons dès aujourd'hui à poser les bases de nos défenses, bien avant d'être dépassés par un avenir post-quantique radieux (mais semé d'embûches).

KEYFACTOR

Keyfactor est la plate-forme d'identité machine et IoT pour l'entreprise moderne. L'entreprise aide les équipes de sécurité à gérer le chiffrement en tant qu'infrastructure critique en simplifiant l'ICP, en automatisant la gestion du cycle de vie des certificats et en permettant l'agilité du chiffrement à l'échelle.

Pour plus d'informations, visitez le site www.keyfactor.com. Vous pouvez également nous suivre sur LinkedIn, Twitter et Facebook.

Fondée sur la confiance et la sécurité, Keyfactor est fière de proposer l'égalité des chances en tant qu'employeur et de soutenir et défendre le développement d'un lieu de travail fiable, sûr, diversifié et inclusif.

Contactez-nous

- www.keyfactor.com
- +1.216.785.2946