4 étapes clés pour vous préparer à la cryptographie post-quantique

On estime que les progrès en matière d'informatique quantique devraient rendre les normes de cryptographie actuelles obsolètes dès 2029[1]. Dans ce contexte, toutes les entreprises seront bientôt contraintes d'appliquer des mécanismes résistant au décryptage basé sur l'informatique quantique. Pour gérer cette menace latente et les attaques (déjà courantes) de type « Harvest now, decrypt later » (collecter maintenant, décrypter plus tard), nous vous proposons ces quatre étapes clés de préparation au cryptage post-quantique.

1 Évaluez les données sensibles et les protocoles de cryptographie existants au sein de votre entreprise

Pour vous préparer à la cryptographie post-quantique, vous devez évaluer la vulnérabilité actuelle des données de votre entreprise.

La meilleure pratique consiste à réunir une équipe pluridisciplinaire (avec des représentants de tous les services concernés, notamment les services informatique, d'exploitation métier, juridique et de la conformité) afin d'identifier et de tracer tous les chemins d'accès à ces données. Les équipes peuvent ainsi commencer à classer les données selon leur vulnérabilité (actuelle, imminente ou future) et d'autres critères.

Ensuite, il est important de faire l'inventaire des protocoles de cryptographie en place et d'identifier ceux qui ont besoin d'être mis à jour le plus rapidement, ceux qui peuvent être modifiés et ceux qui doivent rester identiques en raison de limites matérielles ou logicielles.

2 Identifiez les ressources prioritaires

Maintenant que vos équipes ont dressé un état des lieux des données au sein de votre entreprise, vous pouvez commencer à identifier les ressources à protéger immédiatement.

Il n'est pas pratique, ni même réaliste, de tenter d'assurer la sécurité de toutes vos ressources en même temps. C'est pourquoi il est essentiel d'adopter une approche de planification pragmatique, en vous appuyant sur les informations tirées des travaux préliminaires de vos équipes. L'objectif est d'examiner avec soin les ressources et systèmes à traiter en priorité, et ceux pour lesquels il est possible d'attendre.

1 Horvath, Mark, « Begin Transitioning to Post-Quantum Cryptography Now », Gartner, 30 septembre 2024

3 Commencez à tester de nouveaux algorithmes résistant aux attaques quantiques dans votre environnement

La plupart des organismes de conformité conseillent aux entreprises de commencer à migrer vers de nouveaux protocoles et algorithmes de cryptographie post-quantique dès que possible. C'est notamment le cas du NIST (National Institute of Standards and Technology) dans ses premières normes finalisées publiées en août 2024[2].

Plus tôt vos équipes pourront effectuer des tests et résoudre les problèmes qui pourraient freiner votre transition, mieux votre entreprise sera préparée aux exigences de conformité à venir et pourra réduire les risques liés aux attaques de type « harvest now, decrypt later ».

Pour cette phase de préparation, vous pouvez opter pour l'adoption ou une mise à niveau de Red Hat® Enterprise Linux® 10. Ce système d'exploitation inclut la première génération d'algorithmes résistant aux attaques quantiques, notamment OpenSSL, ML-KEM (FIPS 203) et ML-DSA (FIPS 204), qui assurent l'échange de clés, le cryptage et la signature, ainsi que d'autres fonctionnalités qui devraient être disponibles dans les prochaines versions.

4 Entamez votre transition à grande échelle et passez en production

Bien qu'il s'agisse de l'étape finale, l'implémentation de nouveaux algorithmes résistant aux attaques quantiques est la phase la plus longue et la plus complexe du processus.

Ne vous attendez pas à des résultats immédiats, mais à devoir fournir des efforts soutenus, en gardant les avantages à long terme en tête.

Vous ne pourrez pas mettre à jour chaque algorithme de cryptographie de votre environnement du jour au lendemain. Toutefois, les informations obtenues et les priorités identifiées lors des étapes préliminaires permettront à votre entreprise d'y parvenir à long terme.

Lorsque vous commencerez à apporter des changements à vos protocoles cryptographiques et à intégrer des algorithmes résistant aux attaques quantiques en production, vous devrez porter une attention particulière à toutes les interdépendances identifiées lors de la phase de tests afin de limiter les conséquences involontaires ou les temps d'arrêt.

Commencez dès maintenant votre transition vers la cryptographie post-quantique

Parcourez cette page pour en savoir plus sur la manière dont Red Hat Enterprise Linux 10 intègre des algorithmes résistant aux attaques quantiques afin d'aider votre entreprise à se tenir prête pour l'ère de la cryptographie post-quantique.

2 « NIST Releases First 3 Finalized Post-Quantum Encryption Standards », National Institute of Standards and Technology, 13 août 2024

À propos de Red Hat

Red Hat aide ses clients à standardiser leurs environnements, à développer des applications cloud-native et à intégrer, automatiser, sécuriser et gérer des environnements complexes en offrant des services d'assistance, de formation et de consulting primés.

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

fr.redhat.com

© 2025 Red Hat, Inc. Red Hat et le logo Red Hat sont des marques ou marques déposées de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays. Linux® est la marque déposée de Linus Torvalds aux États-Unis et dans d'autres pays.