Conseils sur la mise en Oeuvre de l'agilité Cryptographique

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

MAI 2020 | ITSAP.40.018

L'agilité cryptographique constitue une pratique exemplaire permettant de changer facilement les algorithmes de chiffrement utilisés dans les applications et les protocoles pour maintenir la sécurité des systèmes malgré la découverte de nouvelles vulnérabilités cryptographiques. Cette pratique repose principalement sur la configuration et ne nécessite pas d'importantes mises à jour logicielles ou matérielles. Les produits agiles doivent être dotés de capacités de mise à niveau logicielle et micrologicielle simplifiées pour gérer les cas où toutes les options de configuration auraient été épuisées. Pour favoriser une transition progressive, les produits agiles doivent maintenir l'interopérabilité avec d'autres systèmes. Ils devraient également conserver la validation des applications et les certifications connexes, en fonction de la configuration. L'agilité repose sur des stratégies et des processus organisationnels qui consistent à tenir un inventaire des emplacements et des cas d'utilisation des algorithmes et produits de chiffrement au sein d'une organisation pour faciliter une transition rapide, simple et complète au besoin.

POURQUOI L'AGILITÉ CRYPTOGRAPHIQUE EST-ELLE IMPORTANTE?

Les percées dans les domaines de la recherche cryptographique et du calcul peuvent affaiblir les algorithmes de chiffrement existants. Les applications héritées utilisent parfois des mécanismes cryptographiques faibles qu'il est difficile de mettre à niveau. Les fournisseurs titulaires de contrats de soutien existants risquent de ne pas être en mesure de réagir assez rapidement pour mettre en œuvre et déployer de nouveaux algorithmes de chiffrement en réponse aux rapports de vulnérabilités et expositions courantes (CVE pour *Common Vulnerabilities and Exposures*).

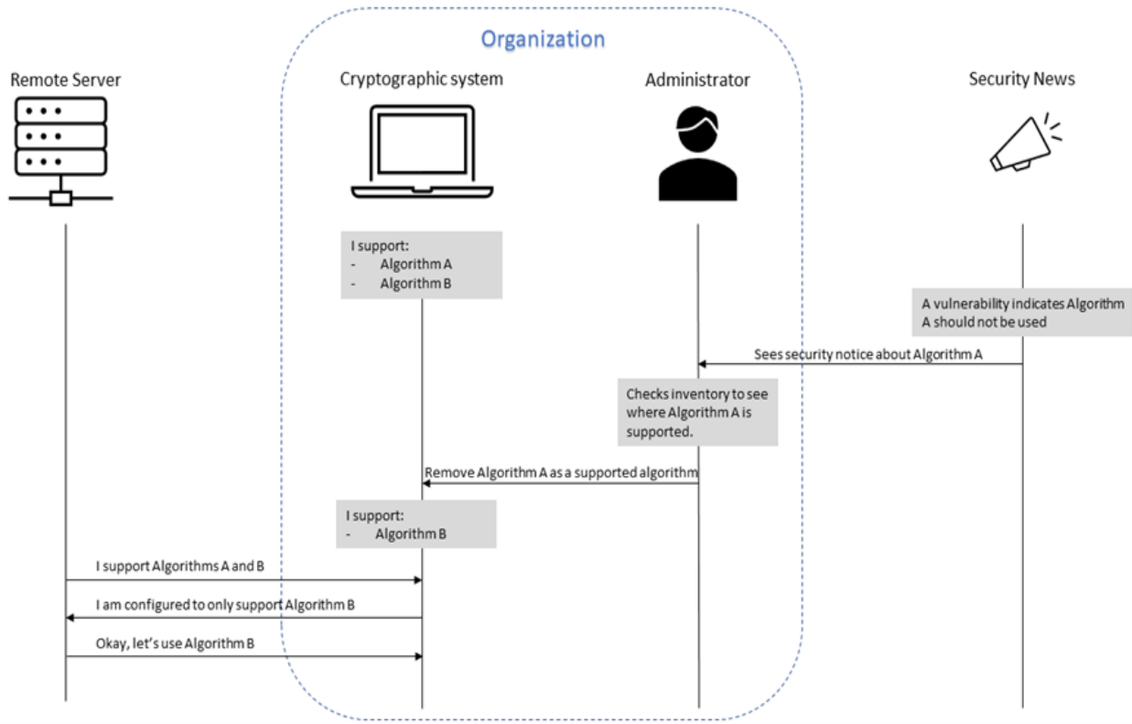
Une importante transition cryptographique est attendue dans un avenir rapproché afin d'atténuer la menace posée par les ordinateurs quantiques. La cryptographie à clé publique utilisée actuellement par les produits d'aujourd'hui serait en grande partie vulnérable à un ordinateur quantique suffisamment puissant. Les produits de cybersécurité qui prennent en charge l'agilité cryptographique peuvent aider votre organisation à traverser cette transition.

EN QUOI CONSISTE L'AGILITÉ CRYPTOGRAPHIQUE?

Les produits de cybersécurité axés sur l'agilité cryptographique ont accès à de multiples algorithmes de chiffrement et permettent aux propriétaires de systèmes de les configurer de manière à utiliser certains algorithmes ou à établir des préférences connexes. Si toutes les options de configuration sont épuisées, ces produits de sécurité comportent des processus simplifiés de mise à niveau logicielle et micrologicielle qui offrent de nouvelles options de configuration. Les systèmes agiles sur le plan de la cryptographie mettent en place des stratégies et des processus qui détectent rapidement les changements apportés à la configuration ainsi que les mises à jour logicielles et micrologicielles.

Les protocoles de sécurité réseau déterminent souvent les algorithmes de chiffrement à employer, ce qui permet de configurer les points terminaux autrement. La capacité de paramétrer les préférences liées aux algorithmes de chiffrement dans les produits permet d'adopter une approche progressive de migration de l'équipement et des applications, ce qui maintient l'interopérabilité.

L'AGILITÉ CRYPTOGRAPHIQUE À L'ŒUVRE



Pour en savoir plus sur la menace quantique, consultez *Faire face à la menace que l'informatique quantique fait peser sur la cryptographie* (ITSE.00.017) et *Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie* (ITSAP.00.017).

Centre de la sécurité des télécommunications
Communications Security Establishment

Canada

L'agilité Cryptographique

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

MAI 2022 | ITSAP.40.018

QUELS MÉCANISMES CRYPTOGRAPHIQUES DEVRAIS-JE MAINTENANT UTILISER?

Avant de faire appel à un fournisseur, assurez-vous que ses produits utilisent des mécanismes cryptographiques normalisés et que la mise en œuvre est certifiée dans le cadre d'un programme d'assurance indépendant (p.ex. Programme de validation des modules cryptographiques [CMVP] et Critères communs [CC]). Le Centre pour la cybersécurité a publié des conseils en matière d'algorithmes de chiffrement et de protocoles dans deux documents : Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (ITSP.40.111) et Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062). Ces documents présenteront des conseils sur la transition vers la cryptographie post-quantique une fois que cette dernière sera normalisée.

MON ORGANISATION EST-ELLE CONFORME À L'AGILITÉ CRYPTOGRAPHIQUE?

Pour déterminer si les produits actuels déployés au sein de votre organisation sont conformes à l'agilité cryptographique, suivez les étapes ci-dessous :

1. Dressez l'inventaire des produits qui utilisent des mécanismes cryptographiques.
2. Demandez à vos fournisseurs de produits comment ils prennent en charge l'agilité cryptographique. S'ils ne la prennent pas en charge, demandez-leur de fournir des précisions sur leurs plans visant à mettre en œuvre l'agilité cryptographique dans de futures versions.
3. Déterminez si les produits agiles actuels et futurs de vos fournisseurs utilisent ou utiliseront des mécanismes cryptographiques normalisés et validés (p. ex. modules validés dans le cadre du Programme de validation des modules cryptographiques).
4. Déterminez si les activités de gestion des changements de TI de votre organisation comportent des stratégies et des procédures qui soutiennent l'agilité cryptographique.

Il peut s'avérer difficile de dresser l'inventaire de tous les mécanismes cryptographiques dans une grande organisation. Certains produits comportent sans doute des mécanismes cryptographiques dont vous n'êtes pas au courant.

Certains fournisseurs offrent des produits qui permettent d'analyser les systèmes et réseaux, puis de générer des rapports sur les mécanismes cryptographiques qu'il faudrait peut-être remplacer. Il convient de tenir compte des considérations habituelles liées à la sécurité et de suivre les pratiques de sécurité nécessaires lors du déploiement d'outils qui surveillent des composants sensibles comme ceux qui emploient des mécanismes cryptographiques.

METTRE EN ŒUVRE L'AGILITÉ CRYPTOGRAPHIQUE

Nous recommandons aux organisations de suivre les étapes ci-dessous pour commencer à mettre en œuvre l'agilité cryptographique :

1. Dresser l'inventaire des produits qui utilisent des mécanismes cryptographiques.
2. Mettre en œuvre de nouvelles stratégies et procédures dans le cadre des activités de gestion des changements de TI pour maintenir cet inventaire et gérer tout changement de configuration lié à l'agilité cryptographique.
3. Demander à vos fournisseurs de produits de chiffrement comment ils prennent en charge l'agilité cryptographique. Comprendre leurs stratégies et procédures de mise à niveau logicielle et micrologicielle liées à toute importante mise à jour nécessaire aux fins d'agilité cryptographique.
4. Élaborer un plan de transition pour tous les produits non agiles, y compris tout mécanisme cryptographique hérité, dans le but de passer à des produits qui prennent en charge l'agilité cryptographique.
5. Établir une politique d'approvisionnement qui veillera à ce que l'agilité cryptographique soit prise en compte lors des futurs achats.
6. S'assurer que le plan d'agilité prévoit l'utilisation d'algorithmes de chiffrement normalisés conformément aux recommandations de l'ITSP.40.111 et de l'ITSP.40.062, et que la mise en œuvre des algorithmes de chiffrement a été validée dans le cadre du Programme de validation des modules cryptographiques.

POUR EN SAVOIR PLUS

Pour obtenir des précisions sur la cybersécurité, consultez les publications suivantes, qui se trouvent sur le site Web du Centre pour la cybersécurité (cyber.gc.ca).

- *Utiliser le chiffrement pour assurer la sécurité des données sensibles (ITSAP.40.016)*
- *Préparez votre organisation à la menace que pose l'informatique quantique pour la cryptographie (ITSAP.00.017)*
- *Les outils de sécurité préventive (ITSAP.00.058)*
- *Directive de mise en œuvre : protection du domaine de courrier (ITSP.40.065)*
- *Facteurs à considérer par les clients de services gérés en matière de cybersécurité (ITSM.50.030)*

Centre de la sécurité des télécommunications
Communications Security Establishment

 No de cat.D97-1/40-018-2022F-PDF ISBN 978-0-660-42979-3

Canada