The 2024 PKI & Digital Trust Report

Tendances et menaces impactant la confiance numérique en 2024

Attention CISOs :

Bienvenue dans l'année de la perturbation numérique !

Voici les points saillants de la nouvelle étude mondiale de Keyfactor qui révèle ce qui affecte vraiment la confiance numérique : une infrastructure à clé publique (PKI) mal gérée, une prolifération de certificats numériques et les changements imminents dans la cryptographie moderne.

La PKI est le fondement de la confiance numérique pour les organisations, fournissant l'authentification et le chiffrement pour tout, des sites web et applications aux appareils IoT et aux charges de travail cloud. Mais l'augmentation de l'utilisation de la PKI pousse les équipes et les outils à leur point de rupture.

Ce que peuvent faire les leaders en sécurité...

Il est temps d'évaluer votre infrastructure PKI et de déterminer si elle peut prendre en charge les cas d'utilisation actuels et, plus important encore, si elle est prête à s'adapter aux changements majeurs à venir.

98% disent qu'ils ont besoin de moderniser leur PKI

La PKI est une infrastructure critique, mais elle devient complexe

+5 Hrs pour identifier et remédier à une panne de certificat

Les interruptions réduisent les revenus (et la confiance).

KEYFACTOR

Les organisations déploient plus que jamais des clés, de certificats et d'identités machine — 91% contre 74% en 2023 et 61% en 2021. Les équipes de sécurité doivent constamment se préoccuper du risque que les équipes d'application et d'exploitation puissent commettre des erreurs ou ignorer les politiques, ce qui entraîne des interruptions perturbatrices. Le rapport montre qu'en moyenne, il faut plus de 5 heures aux équipes pour identifier et remédier à une panne de certificat. Il est temps d'investir dans la visibilité et l'automatisation. Heureusement, les répondants ont indiqué que c'était une priorité absolue pour l'année à venir.

Ce que peuvent faire les leaders en sécurité...

Les interruptions causées par des certificats expirés ont un impact sérieux sur la confiance des clients, les revenus et la productivité des employés, surtout lorsqu'elles affectent les systèmes orientés vers l'extérieur. Les leaders en sécurité doivent comprendre la gravité et la fréquence des interruptions et donner la priorité à la capacité de leur équipe à prévenir et à répondre à ces incidents.

95% rencontrent des obstacles en préparant la cryptographie post-quantique

Le quantum computing se profile à l'horizon

Prêts ou non, l'informatique quantique arrive, et les organisations doivent se préparer en adoptant la cryptographie post-quantique (PQC). Les acteurs malveillants ont déjà commencé à récolter et stocker des données chiffrées dans le but de les déchiffrer lorsque sera disponible un ordinateur quantique suffisamment puissant pour briser le chiffrement moderne.

Ce que peuvent faire les leaders en sécurité...

Il est temps de commencer à planifier votre feuille de route vers la sécurité quantique – cela commence par obtenir une visibilité sur vos données et actifs cryptographiques.

Vous voulez en savoir encore plus sur les tendances et les menaces principales ?

Téléchargez ""The 2024 PKI & Digital Trust Report"" de Keyfactor et obtenez de nouvelles idées pour améliorer la sécurité, la fiabilité et l'intégrité des interactions numériques de votre organisation.

Download now ↗