yubico

YubiKey, la MFA résistante au phishing

Sécurise les stations de travail partagées contre les cyberattaques modernes

L'authentification d'ancienne génération expose votre entreprise à des risques

La nature même des stations de travail partagées en fait des cibles de choix pour les cyberdélinquants et les initiés, ce qui amplifie les risques associés aux appareils, aux accès des utilisateurs et à l'authentification.

L'authentification multi-facteurs (MFA) peut procurer une première ligne de défense solide pour protéger ceux qui utilisent des stations de travail et des appareils partagés contre les cyberattaques modernes, mais toutes les méthodes de MFA ne se valent pas. L'authentification d'ancienne génération avec un nom d'utilisateur et un mot de passe peut être facilement piratée, et l'authentification basée sur les appareils mobiles, notamment par SMS, code OTP et notifications push est fortement exposée aux attaques modernes par hameçonnage, aux malwares, aux échanges de SIM et aux attaques de l'homme du milieu (MiTM). En plus de la sécurité, il est également important de prendre en considération l'expérience utilisateur, la portabilité et l'évolutivité des solutions d'authentification. De mauvaises expériences utilisateur, une faible portabilité et un manque d'évolutivité peuvent entraîner des failles dans la MFA, une faible adoption par les utilisateurs et un risque accru de violation des données.

Bornes partagées

Les bornes partagées supportent souvent de multiples utilisateurs en un seul service, ce qui augmente la prévalence de pratiques non sécurisées autour du partage de mot de passe pour tenter de réduire les délais de connexion/déconnexion.

Limitations des appareils mobiles

Les stations de travail et les appareils partagés dans des environnements où les appareils mobiles ne sont pas autorisés requièrent une authentification hautement sécurisée, conforme aux réglementations du secteur et intuitive.

Prêt à l'emploi

Étant donné que, dans ce scénario, aucun utilisateur n'est lié à un appareil en particulier, il est important que des contrôles permettent de donner rapidement et simplement accès uniquement aux applications et services associés aux identifiants d'un utilisateur en particulier.

Terminaux de points de vente (POS)

Une attention particulière doit être apportée à la vitesse et à la facilité d'authentification sur les terminaux POS, pour éviter les verrouillages potentiels des comptes, et plus important encore, pour s'assurer de la sécurité ainsi que de la conformité des informations des paiements avec les normes PCI DSS.

Éléments essentiels pour sécuriser les stations de travail partagées

Lorsqu'elles cherchent des solutions d'authentification pour des stations de travail partagées, en plus de savoir si une solution protège efficacement contre les cyberattaques externes et les menaces internes, les entreprises devraient également se demander si la solution a un impact sur la productivité de l'utilisateur (verrouillage du compte, délai de connexion), si elle est fiable pour des environnements et des cas d'usage variés, notamment car des variables externes peuvent affecter la performance comme la qualité du réseau et la batterie, mais aussi quel serait le coût final sur le long terme.

Sécurité

Comment être sûr que l'utilisateur qui se connecte à l'appareil est bien un utilisateur légitime ?

Efficacité

Comment être sûr que l'utilisateur peut s'authentifier facilement sur plusieurs appareils ?

Fiabilité

Comment garantir une authentification cohérente qui fonctionne sans interruption, y compris dans des environnements difficiles avec des degrés variés de connexion ?

Coût

Comment réduire le nombre de tickets d'assistance liés à l'authentification ?

La série YubiKey 5

De gauche à droite : YubiKey 5 NFC, YubiKey 5C NFC, YubiKey 5Ci, YubiKey 5C, YubiKey 5 Nano et YubiKey 5C Nano

La série YubiKey 5 CSPN

De gauche à droite : YubiKey 5 NFC CSPN, YubiKey 5C NFC CSPN, YubiKey 5Ci CSPN, YubiKey 5C CSPN, YubiKey 5 Nano CSPN et YubiKey 5C Nano CSPN

Sécuriser les stations de travail partagées avec la YubiKey

Yubico propose la YubiKey, une clé matérielle de sécurité dans un format USB et nano portable, idéale pour les environnements où les stations de travail sont partagées. La YubiKey procure une authentification forte à deux facteurs, multi-facteurs, sans mot de passe et résistante au phishing, en fonction des besoins, grâce à un authentificateur physique permettant de protéger les secrets privés sur un élément sécurisé qui ne peut pas être facilement exfiltré. D'après des recherches indépendantes, la YubiKey est la seule solution ayant réussi à arrêter 100 % des usurpations de comptes.[1]

Grâce à la YubiKey, les utilisateurs peuvent s'authentifier facilement et en toute sécurité sur plus de 700 applications et services sur divers appareils, d'une seule touche : aucune installation de logiciel, aucune batterie et aucune connexion cellulaire ne sont nécessaires. La YubiKey utilise les protocoles d'authentification modernes tels que les standards d'authentification FIDO U2F et FIDO2 pour aider à éliminer les attaques par phishing ciblant les identifiants. Les YubiKey sont également compatibles avec la technologie carte à puce, OTP et les protocoles OpenPGP, ce qui permet d'utiliser une seule clé de sécurité sur divers systèmes modernes et d'ancienne génération.

	Nom d'utilisateur et mot de passe	Authentificateurs basés sur des appareils mobiles	YubiKey
Sécurité	Faible, facilement piraté	Moyen, 10-50 % de taux d'usurpations de comptes[2]	Haut, 0 % de taux d'usurpation de comptes[3]
Efficacité	Fatigue liée aux mots de passe, verrouillage des comptes	Les utilisateurs qui ne peuvent pas, ne veulent pas et n'utilisent pas le MFA mobile	Expérience consistant à taper sur une touche. Connexion 4 fois plus rapide qu'un OTP[4]
Fiabilité	Sujets aux erreurs humaines	Dépendent d'un appareil ayant une batterie et d'un réseau cellulaire Pas adaptés aux environnements limités aux appareils mobiles	Construction solide, ne s'appuyant pas sur le réseau cellulaire
Coût	Pas de coûts initiaux Coût élevé de l'assistance informatique Risque potentiel élevé	1 840 $, c'est le vrai coût de la mobilité de l'entreprise pour chaque appareil détenu[5]	Un coût faible par rapport au MFA mobile, et 92 % de tickets d'assistance en moins[6]

[1] Google, New research: How effective is basic account hygiene at preventing account takeovers

[2-4] Ibid

[5] Wander: Uncovering the true costs of enterprise mobility

[6] Google, New research: How effective is basic account hygiene at preventing account takeovers

Yubico (Nasdaq First North Growth Market Stockholm : YUBICO) est l'inventeur de la YubiKey, la référence en matière d'authentification multi-facteurs (MFA) résistante au phishing, et un créateur et contributeur des standards d'authentification ouverts FIDO. L'entreprise est un pionnier de l'authentification par passkeys matérielles, avec des clients dans plus de 160 pays. Pour en savoir plus, rendez-vous sur www.yubico.com.

© 2023 Yubico