yubico

Google se défend contre les piratages de comptes et réduit les coûts informatiques

Les clés YubiKey protègent les employés de Google depuis 2009

Étude de cas

Google

Industrie
Technologie

Protocoles
U2F

Produits
Tous les facteurs de forme YubiKey

Déploiement
Employés

U2F pour USB

À propos de Google

En 1998, Google a été fondé avec une mission : organiser les informations du monde et les rendre universellement accessibles et utiles. Depuis lors, la société s'est concentrée sur le développement de services visant à améliorer de manière importante la vie du plus grand nombre de personnes possible, et aujourd'hui, Google est une société mondiale du classement Fortune 50 considérée comme l'une des principales sociétés Internet dans le monde. Pour une entreprise technologique innovante, telle que Google, la nécessité de s'assurer que l'accès en ligne aux informations confidentielles est limité aux employés et aux sous-traitants approuvés est essentielle à la réussite de l'entreprise.

Surmonter les piratages de comptes

En 2009, Google a été la cible de cyberattaques sophistiquées capables de contourner les contrôles de sécurité traditionnels. En l'absence d'options d'authentification à deux facteurs (2FA) viables pour empêcher efficacement ces attaques et les piratages de comptes, Google a commencé à travailler en étroite collaboration avec Yubico pour étendre les capacités de la technologie d'authentification à deux facteurs de la YubiKey afin d'inclure également la crytopgraphie à clé publique. Grâce à cette collaboration, Yubico et Google ont cocréé un protocole d'authentification forte basé sur le concept d'une clé unique résistante au phishing (hameçonnage) pour sécuriser tous les services. C'est ce travail qui est devenu par la suite une norme ouverte adoptée par l'alliance FIDO appelée la norme FIDO Universal 2nd Factor (U2F).

Une seule clé YubiKey peut sécuriser une multitude de services en ligne sans qu'aucune information utilisateur ou clé privée ne soit partagée entre les fournisseurs de services. Il n'y a aucune dépendance ou exigence en matière de connectivité mobile, de périphériques cellulaires, d'applications mobiles ou de saisie manuelle de codes.

Résultats

Après deux ans d'évaluation des mots de passe à usage unique (OTP), des certificats TLS, des cartes à puce et d'autres méthodes d'authentification, Google a confirmé que les Security Keys FIDO U2F étaient les mieux adaptées pour répondre aux besoins de l'entreprise en matière de sécurité et de convivialité. Peu de temps après, Google a étendu son déploiement de la clé YubiKey à l'ensemble de son personnel et de ses sous-traitants pour une connexion sécurisée aux ordinateurs et aux serveurs, atteignant ainsi plus de 50 000 employés à ce jour.

L'étude de deux ans menée par Google pour mesurer l'impact commercial de l'authentification matérielle a mis en évidence plusieurs avantages importants :

Sécurité renforcée : Les comptes internes protégés uniquement par une clé YubiKey et FIDO U2F ont connu une augmentation importante du niveau de sécurité.

Accélération de la productivité des employés : Les employés ont constaté une réduction significative, de près de 50 %, du temps d'authentification à l'aide d'une clé YubiKey par rapport à l'utilisation d'un mot de passe à usage unique (OTP) par SMS. Les connexions étaient presque quatre fois plus rapides en comparant la clé YubiKey à l'Authentificateur de Google (Google Authenticator). Le gain de temps est principalement dû à l'authentification à la YubiKey d'un simple toucher qui s'exécute en quelques millisecondes.

Étude de cas

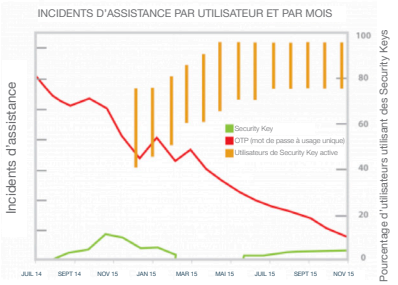
Google

Industrie
Technologie

Protocoles
U2F

Produits
Tous les facteurs
de forme YubiKey

Déploiement
Employés



Diminution de l'assistance : Par rapport à l'utilisation d'un téléphone pour l'authentification, les clés YubiKey se sont révélées être faciles à utiliser, robustes dans leur conception, imperméables et ne se cassent pas facilement. La clé YubiKey a également permis de fournir plusieurs solutions de sauvegarde à chaque employé, y compris une clé YubiKey nano conçue pour être présente à l'intérieur de l'ordinateur portable de l'utilisateur et une clé YubiKey conçue pour un porte-clés. Google a constaté une baisse des appels d'assistance, avec une réduction de 92 % des incidents d'assistance, ce qui permet d'économiser des milliers d'heures par an en frais d'assistance. De plus, les échecs d'authentification sont estimés à zéro.

Coût de propriété réduit : La combinaison de la sécurité, de la convivialité et de l'efficacité du flux de travail de la clé YubiKey a permis à Google de donner à chaque employé plusieurs clés YubiKey tout en réalisant néanmoins des réductions globales de coûts.

Protéger les employés et les clients grâce à une forte 2FA

Aujourd'hui, Google ne protège pas seulement ses employés avec la clé YubiKey, mais a également intégré la prise en charge de la clé YubiKey et des clés de sécurité FIDO U2F dans les protections de sécurité disponibles pour tous les utilisateurs de Google. Tout utilisateur possédant un compte Google peut désormais se protéger contre le phishing avancé et bénéficier de l'authentification forte fournie par la clé YubiKey.

La plus forte défense contre le phishing

Plus récemment, en octobre 2017, Google a lancé son programme de protection avancée (GAPP) pour les utilisateurs les plus à risque, notamment les journalistes, les chefs d'entreprise et les équipes de campagne politique. Le programme GAPP renforce encore la sécurité des utilisateurs de comptes Google en exigeant l'utilisation de clés de sécurité FIDO U2F pour une connexion sécurisée, au lieu de les rendre optionnelles. Pour fournir la défense la plus forte contre le phishing, la protection avancée va au-delà de la traditionnelle vérification en 2 étapes. Les participants au programme GAPP sont tenus de se connecter à leur compte avec un mot de passe et une clé de sécurité physique, c'est-à-dire la clé YubiKey. D'autres facteurs d'authentification, y compris les codes envoyés par SMS ou l'application Google Authenticator, ne fonctionneront plus, car il a été démontré que ces formes de 2FA sont susceptibles d'être hameçonnées (phishable).

Protection des clients Adwords

Google a également souligné les avantages de la protection des comptes Adwords avec la clé YubiKey. En 2016, Google a publié un blog soulignant la façon dont deux agences de marketing numérique, Jellyfish et iProspect, protègent leurs comptes AdWords, leurs clients et leurs revenus en utilisant la clé YubiKey.

Authentification moderne à grande échelle

Google est une entreprise technologique de premier plan et l'innovation et l'invention sont au cœur de son activité. En collaboration avec Yubico, Google a joué un rôle essentiel dans la définition de la norme ouverte pour l'authentification forte, désormais connue sous le nom de norme FIDO U2F. Aujourd'hui, Yubico et Google offrent à plus d'un milliard d'utilisateurs de Gmail et à plus de 50 000 employés de Google une authentification forte à deux facteurs résistante au phishing pour protéger les données personnelles et sécuriser l'accès à Internet. Les clés de sécurité n'ont conduit à aucun piratage de comptes confirmé et ont augmenté le degré de satisfaction des utilisateurs depuis le déploiement à grande échelle.

Mayank Upadhyay, directeur de l'ingénierie de la sécurité, Google Inc.

« Nous estimons qu'en utilisant cette clé, nous avons élevé le niveau de sécurité pour nos employés au-delà de ce qui était disponible sur le marché. Le périphérique fonctionne avec le navigateur Web Chrome de Google, et fonctionne de façon très transparente pour les personnes dans leur travail quotidien ici chez Google. »

À propos de Yubico Yubico établit de nouvelles normes mondiales pour un accès facile et sécurisé aux ordinateurs, serveurs et comptes Internet. Fondée en 2007, Yubico est une entreprise privée qui possède des bureaux en Australie, en Allemagne, à Singapour, en Suède, au Royaume-Uni et aux États-Unis. Découvrez pourquoi neuf des 10 plus grandes marques Internet et des millions d'utilisateurs dans plus de 160 pays utilisent notre technologie sur www.yubico.com.

Yubico AB
Kungsgatan 44
2nd floor
SE-111 35 Stockholm
Sweden

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 États-Unis
844-205-6787 (numéro vert)
650-285-0088