yubico

Google se defiende de la suplantación de cuentas y reduce los costes de TI

YubiKey protege a los empleados de Google desde 2009

Caso práctico

Google

Sector
Tecnología

Protocolos
U2F

Productos
Todas las YubiKeys

Implementación
Empleados

U2F para USB

Acerca de Google

Google se fundó en 1998 con una misión: organizar la información del mundo y hacerla accesible y útil a escala universal. Desde entonces, la empresa se ha centrado en el desarrollo de servicios para mejorar de forma significativa la vida del mayor número de personas y, hoy en día, Google es una empresa global de la lista Fortune 50 considerada como una de las empresas de internet líder mundial. Para una empresa de tecnología innovadora como Google, la necesidad de garantizar que el acceso en línea a la información confidencial esté restringido a los empleados y contratistas autorizados es fundamental para su éxito.

Detener la suplantación de cuentas

En 2009 Google fue objeto de sofisticados ciberataques capaces de burlar los controles de seguridad tradicionales. Ante la falta de opciones viables de autenticación de dos factores (2FA) para evitar estos ataques y la suplantación de cuentas de forma eficaz, Google comenzó a trabajar en estrecha colaboración con Yubico para ampliar las prestaciones de la tecnología de autenticación de dos factores de YubiKey e incluir también la criptografía de clave pública. A través de esta colaboración, Yubico y Google crearon un protocolo de autenticación segura basado en el concepto de una única llave física resistente al phishing para proteger todos los servicios. Este trabajo fue el que más tarde se convirtió en el estándar abierto adoptado por la alianza FIDO llamado protocolo universal de dos factores, o FIDO U2F.

Una sola YubiKey puede proteger muchos servicios en línea sin compartir información de usuario o las claves privadas entre los proveedores de servicios. No existe una dependencia o requisito de conectividad móvil, dispositivos móviles, aplicaciones móviles o introducción manual de códigos.

Resultados

Tras una evaluación de dos años utilizando contraseñas de un solo uso (OTP), certificados TLS, tarjetas inteligentes y otros métodos de autenticación, Google confirmó que las llaves de seguridad FIDO U2F eran las más adecuadas para satisfacer las necesidades de la empresa en materia de seguridad y facilidad de uso. Poco después, Google amplió la implementación de YubiKeys a todo el personal y a los contratistas para el acceso seguro a ordenadores y servidores, llegando a más de 100 000 empleados globalmente hasta la fecha.

El estudio de estos dos años realizado por Google para medir el impacto empresarial de la autenticación basada en hardware puso de manifiesto varias ventajas importantes:

Incremento de la seguridad: las cuentas internas protegidas únicamente con YubiKey y FIDO U2F experimentaron un aumento significativo en el nivel de seguridad.

Incremento de la productividad de los empleados: los empleados vieron una reducción significativa, de casi el 50 %, del tiempo de autenticación usando una YubiKey en comparación con el uso de una contraseña de un solo uso (OTP) a través de SMS. Los inicios de sesión fueron casi cuatro veces más rápidos cuando se comparó YubiKey con Google Authenticator. El ahorro de tiempo se debe principalmente a la autenticación con un solo toque de YubiKey que se ejecuta en milisegundos.

Caso práctico

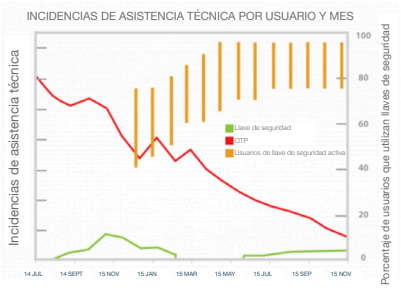
Google

Sector
Tecnología

Protocolos
U2F

Productos
Todas las YubiKeys

Implementación
Empleados



Menor soporte: en comparación con el uso de un teléfono para la autenticación, se descubrió que la YubiKey era más fácil de usar, con un diseño sólido, resistente al agua y que no se rompía fácilmente. También fue posible repartir varias llaves de seguridad para cada empleado, incluida una YubiKey nano diseñada para colocarse en el portátil del usuario y una YubiKey transportable diseñada para llevar en el llavero. Google descubrió que las llamadas a soporte técnico se redujeron, con una reducción del 92 % en las incidencias de soporte, lo que ahorró miles de horas al año en costes de asistencia. Además, se estima que los fallos de autenticación se han reducido a cero.

Menor coste de propiedad: la combinación de seguridad, facilidad de uso y eficiencia en el flujo de trabajo de YubiKey permitió a Google dar a cada empleado varias YubiKeys y aun así realizar reducciones de costes generales.

Proteja a sus empleados y clientes con una 2FA segura

Hoy en día, Google no solo protege a sus empleados con YubiKeys, sino que también ha integrado la compatibilidad con las llaves de seguridad YubiKey y FIDO U2F en las protecciones de seguridad disponibles para todos los usuarios de Google. Cualquier usuario con una cuenta de Google puede protegerse del phishing avanzado y beneficiarse de la autenticación segura que ofrece YubiKey.

La mejor defensa contra el phishing

Más recientemente, en octubre de 2017, Google lanzó su Programa de Protección Avanzada (GAPP) para aquellos usuarios de mayor riesgo, como periodistas, líderes empresariales y equipos de campañas políticas. El programa GAPP refuerza aún más la seguridad de los usuarios de cuentas de Google al hacer obligatorio, en lugar de opcional, el uso de llaves de seguridad FIDO U2F respaldadas por hardware para iniciar sesión de forma segura. Para ofrecer la defensa más segura contra el phishing, la protección avanzada va más allá de la tradicional verificación en dos pasos. Los participantes del programa GAPP deben entrar en su cuenta con una contraseña y una llave de seguridad física, es decir, una YubiKey. Otros factores de autenticación, incluidos los códigos enviados por SMS o la aplicación Google Authenticator, dejan de funcionar, ya que se ha demostrado que estas formas de 2FA pueden ser objeto de phishing.

Protección de los clientes de Adwords

En 2016, Google publicó una entrada de blog en la que se destacaba cómo dos agencias de marketing digital, Jellyfish e iProspect, protegen las cuentas de AdWords, los clientes y los ingresos con YubiKey.

Autenticación moderna a escala

Google es una empresa tecnológica líder con la innovación y la invención como eje central. Al trabajar en colaboración con Yubico, Google fue decisiva en la definición del estándar abierto para la autenticación segura que ahora se conoce como el estándar FIDO U2F. Hoy en día, Yubico y Google ofrecen a más de mil millones de usuarios de Gmail y a más de 100.000 empleados de Google una autenticación segura de dos factores resistente al phishing para proteger los datos personales y el acceso seguro a internet. Gracias a las llaves de seguridad ya no se han registrado más suplantaciones de cuentas y desde su implementación masiva los empleados están más satisfechos.

Mayank Upadhyay, director de ingeniería de seguridad, Google Inc.

«Creemos que al utilizar este token hemos elevado el estándar de seguridad para nuestros empleados más allá de lo que era posible a nivel comercial. El dispositivo funciona con el navegador web Google Chrome y es la mejor opción para el flujo de trabajo diario de los empleados de Google».

Yubico AB
Kungsgatan 44
2 ° piso
SE-111 35 Estocolmo
Suecia

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 EE. UU.
844-205-6787 (número gratuito)
650-285-0088