yubico

Google schützt sich vor Kontendiebstahl und verringert IT-Kosten

Seit 2009 schützen YubiKeys die Mitarbeiter von Google

Fallstudie

Google

Branche
Technologieunternehmen

Protokolle
U2F

Produkte
Alle YubiKey-Formfaktoren

Einsatzbereich
Mitarbeiter

U2F für USB

Über Google

Google wurde 1998 mit einer Mission im Sinn gegründet: die Informationen der Welt zu ordnen und sie für jeden zugänglich und nutzbar zu machen. Seitdem konzentriert sich das Unternehmen auf die Entwicklung von Onlinediensten, die das Leben von so vielen Menschen wie möglich signifikant verbessern sollen. Heute zählt Google zu den weltweiten „Fortune 50“-Unternehmen und gilt als eine der führenden Internet-Firmen der Welt. Für einen Anbieter innovativer Technologien wie Google ist es von entscheidender Bedeutung für den Erfolg, dass der Online-Zugang zu vertraulichen Informationen nur berechtigten Angestellten und Vertragspartnern offensteht.

Das Ende des Kontendiebstahls

2009 war Google das Ziel komplexer Cyberangriffe, bei denen herkömmliche Sicherheitskontrollen umgangen wurden. Da Google die Möglichkeit einer brauchbaren Zwei-Faktor-Authentifizierung (2FA) zur effektiven Verhinderung dieser Angriffe und Kontoübernahmen fehlte, begann die enge Zusammenarbeit mit Yubico. Ziel war es, die Zwei-Faktor-Authentifizierung des YubiKey um Kryptographie mit öffentlichem Schlüssel zu erweitern. Durch diese Zusammenarbeit haben Yubico und Google gemeinsam ein starkes Authentifizierungsprotokoll auf Grundlage eines einzelnen Phishing-resistenten Schlüssels für alle Geräte entwickelt. Das Ergebnis wurde später ein offener Standard, der von der FIDO-Allianz übernommen und „FIDO Universal 2nd Factor (U2F)“ getauft wurde.

Mit einem einzigen YubiKey lassen sich mehrere Onlinedienste sichern, ohne dass Benutzerinformationen oder private Schlüssel zwischen den Anbietern der Dienste ausgetauscht werden. Es ist keine mobile Konnektivität erforderlich, keine mobilen Geräte, Apps oder eine manuelle Code-Eingabe.

Ergebnisse

Nach einer zweijährigen Testphase mit Einmalkennwörtern (OTPs, one-time passwords), TLS-Zertifikaten, Smart Cards und anderen Authentifizierungsmethoden bestätigte Google, dass FIDO U2F-Sicherheitsschlüssel am besten die Anforderungen des Unternehmens an Sicherheit und Benutzerfreundlichkeit erfüllen. Kurz darauf erhielten alle Mitarbeiter und Vertragspartner von Google einen YubiKey für die sichere Anmeldung an Computern und auf Servern. Heute sind so über 50.000 Mitarbeiter damit versorgt.

Bei der zweijährigen Studie über die betriebswirtschaftlichen Auswirkungen der hardwarebasierten Authentifizierung wurden mehrere Vorteile deutlich:

Verbesserte Sicherheit: Interne Konten, die allein mit einem YubiKey und FIDO U2F geschützt waren, wurden wesentlich sicherer.

Gesteigerte Produktivität der Mitarbeiter: Die Mitarbeiter stellten eine signifikante Verringerung der Authentifizierungszeit von fast 50 % fest, wenn sie den YubiKey anstelle eines Einmalkennworts per SMS nutzten. Der Anmeldevorgang verlief mit dem YubiKey nahezu vier Mal so schnell wie mit dem Google Authenticator. Die Zeitersparnis ist vor allem auf die Authentifizierung per Antippen des YubiKey zurückzuführen, die innerhalb von Millisekunden erfolgt.

Fallstudie

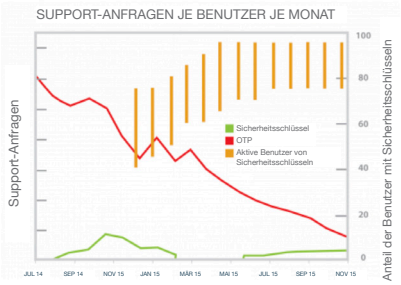
Google

Branche
Technologieunternehmen

Protokolle
U2F

Produkte
Alle YubiKey-Formfaktoren

Einsatzbereich
Mitarbeiter



Weniger Support erforderlich: Im Vergleich mit der Authentifizierung per Telefon wurden YubiKeys als einfach anzuwenden, robust, wasserdicht und nicht leicht zu zerstören wahrgenommen. Der YubiKey ermöglichte auch die Ausgabe mehrerer Backups für jeden Mitarbeiter, darunter auch ein YubiKey nano, der sich im Laptop des Benutzers befindet, sowie ein YubiKey, der an ein Schlüsselbund gehängt werden kann. Google stellte einen Rückgang der Support-Anfragen von 92 % fest – eine Ersparnis von tausenden Stunden an Support-Kosten jedes Jahr. Des Weiteren wird geschätzt, dass die Zahl der fehlgeschlagenen Authentifizierungsversuche bei null liegt.

Niedrige Betriebskosten: Die Effizienz in Bezug auf Sicherheit, Benutzerfreundlichkeit und Workflow durch den YubiKey erlaubte es Google, jedem Mitarbeiter mehrere YubiKeys zur Verfügung zu stellen und dennoch die Kosten unterm Strich zu senken.

Schutz von Mitarbeitern und Kunden mit starker 2FA

Heute schützt Google nicht nur seine Mitarbeiter mit dem YubiKey, sondern stellt auch allen Google-Nutzern die integrierte Unterstützung für die YubiKeys und FIDO U2F-Sicherheitsschlüssel als Sicherheitsmaßnahme zur Verfügung. Jeder Benutzer mit einem Google-Konto kann sich jetzt mit der starken Authentifizierung durch den YubiKey selbst vor komplexen Phishing-Angriffen schützen.

Der stärkste Schutz gegen Phishing

Im Oktober 2017 startete Google sein Advanced Protection-Programm (GAPP) für alle Benutzer mit erhöhtem Sicherheitsrisiko, darunter Journalisten, Geschäftsführer sowie für politische Kampagnen. Durch das Programm „GAPP“ wird die Sicherheit für Nutzer von Google-Konten noch erhöht, indem Hardware-Sicherheitsschlüssel mit FIDO U2F für diese Benutzer verpflichtend werden. Um den maximalen Schutz vor Phishing zu bieten, geht die Advanced Protection noch über die herkömmliche Zwei-Schritt-Verifizierung hinaus. Die Teilnehmer am GAPP-Programm müssen sich in ihrem Konto mit einem Kennwort plus physischem Sicherheitsschlüssel, dem YubiKey, anmelden. Andere Authentifizierungsfaktoren wie SMS-Codes oder die App „Google Authenticator“ funktionieren nicht mehr, da sich gezeigt hat, dass diese Formen der Zwei-Faktor-Authentifizierung anfällig für Phishing sind.

Schutz von AdWords-Kunden

Google hebt auch die Vorteile des Schutzes von AdWords-Konten mit dem YubiKey hervor. 2016 veröffentlichte Google einen Blogeintrag, aus dem hervorgeht, wie zwei digitale Marketingagenturen, Jellyfish und iProspect, ihre AdWords-Konten, -Kunden und -Umsätze mit dem YubiKey schützen.

Moderne Authentifizierung in großem Maßstab

Google ist ein führendes Technologieunternehmen, bei dem Innovation und Erfindergeist im Zentrum stehen. Bei der Zusammenarbeit mit Yubico hat Google den offenen Standard für die starke Authentifizierung, die heute als der Standard „FIDO U2F“ bekannt ist, entscheidend geprägt. Heute bieten Yubico und Google starke Zwei-Faktor-Authentifizierung mit Phishing-Schutz für über eine Milliarde Gmail-Nutzer und über 50.000 Google-Mitarbeiter, um den Schutz persönlicher Daten und den sicheren Zugang zum Internet sicherzustellen. Dank der Sicherheitsschlüssel gab es seit der großflächigen Einführung keine bestätigten Fälle von Kontoübernahmen bei zugleich gesteigerter Kundenzufriedenheit.

> Mayank Upadhyay, Director of Security Engineering, Google Inc.
>
> „Wir glauben, mit der Nutzung dieses Tokens den Standard für die Sicherheit unserer Mitarbeiter über das damals marktübliche Niveau gehoben zu haben. Das Gerät kann mit dem Webbrowser Chrome von Google verwendet werden und lässt sich praktisch nahtlos im täglichen Workflow hier bei Google einsetzen.“

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

Yubico Inc.
530 Lytton Avenue, Suite 301
Palo Alto, CA 94301 USA
844-205-6787
650-285-0088