

Google försvarar sig mot kontotjuvar och minskar IT-kostnader

YubiKeys skyddar Google-anställda sedan 2009

Fallstudie



Branschen

Teknik

Protokoll

U2F

Produkter

Alla YubiKeys
formulärfaktorer

Spridning

Anställda

U2F för USB



Om Google

Google grundades 1998 med missionen att organisera världens information och göra den tillgänglig och användbar. Sedan dess har företaget fokuserat på att utveckla tjänster som påtagligt förbättrar livet för så många människor som möjligt och idag är Google en global framgångssaga med plats på Fortune 500-listan och anses vara ett av de ledande internetföretagen i världen. För ett innovativt, tekniskt företag som Google är det livsviktigt för framgången att tillgången online till konfidentiell information är begränsad till godkända anställda och leverantörer.

Vinna över kontotjuvar

2009 var Google målet för sofistikerade cyberattacker med kapacitet att kringgå traditionella säkerhetskontroller. I brist på möjligheter till en livskraftig verifiering med två faktorer (2FA) som effektivt kunde hindra dessa attacker och kontotjuvar, startade Google ett tätt samarbete med Yubico för att utöka kapaciteten hos YubiKeys verifieringsteknologi med två faktorer till att också inkludera kryptering av offentliga nycklar. Genom detta samarbete skapade Yubico och Google ett starkt verifieringsprotokoll baserat på ett koncept med en enhetlig, nätfiskeresistent nyckel som skulle kunna skydda alla tjänster. Det är detta arbete som senare blev en öppen standard som anammades av den FIDO-allians som kallas FIDO Universal 2nd Factor (U2F) standard.

En enda YubiKey kan skydda en mångfald av onlinetjänster utan att någon användarinformation eller privata nycklar delas mellan de olika leverantörerna. Det finns inget stöd för eller krav på mobil uppkoppling, mobiltelefoner, mobilappar eller manuella kodlås.

Resultat

Efter två års utvärdering av engångslösenord (OTP:s), TLS-certifikat, smarta kort och andra verifieringsmetoder, bekräftade Google att FIDO U2F Security Keys var bäst lämpade att leverera enligt företagets behov av säkerhet och användbarhet. Kort därefter utökade Google sin spridning av YubiKey för ett ge alla anställda och leverantörer säker inloggning på datorer och servrar. Hittills omfattas mer än 50 000 anställda.

Googles tvååriga studie för att mäta affärsnyttan av hårdvarubaserad verifiering visar flera viktiga fördelar:

Ökad säkerhet: Interna konton som skyddas enbart med en YubiKey och FIDO U2F har uppvisat en märkbar ökning av säkerhetsnivån..

Tilltagande produktivitet bland anställda: Anställda upplevde en markant minskning - nästan 50 procent - av tiden för verifiering med hjälp av YubiKey jämfört med vid användning av engångslösenord (OTP) via SMS. Inloggning går nästan fyra gånger snabbare med YubiKey än med Google Authenticator. Tidsbesparingen beror främst på YubiKeys verifiering med ett enda klick, vilket bara tar millisekunder.

Fallstudie



Branschen

Teknik

Protokoll

U2F

Produkter

Alla YubiKeys
formulärfaktorer

Spridning

Anställda

Minskad support: Jämfört med att använda en telefon för verifiering visade sig YubiKeys vara enkla att hantera med sin robusta design, vattentät och hållbarhet. YubiKey tillåter också backuper i olika former till varje anställd. Ett exempel är en YubiKey i nanoformat, som kan fästas användarens laptop samt en YubiKey som är designad för en nyckelkedja. Google märkte även att supportsamtalet minskade, bland annat minskade supportincidenterna med 92 procent, vilket sparar tusentals timmar per år i supportkostnader. Dessutom uppskattas antalet verifieringsfel till noll.

Minskade kostnader för ägande: Kombinationen av säkerhet, användbarhet och effektivisering av arbetsflödet gjorde att Google kunde ge alla anställda ett antal YubiKeys och ändå göra övergripande kostnadsminskningar.

Skydda anställda och kunder med starkt 2FA

Idag är det inte bara så att Google skyddar anställda med YubiKey utan de har också integrerat support för säkerhetsnycklar från YubiKey och FIDO U2F i de tillgängliga säkerhetsskydden för alla Google-användare. Alla användare med ett Google-konto kan nu skydda sig själva från avancerat nätfiske och dra nytta av den starka verifieringen som tillhandahålls av YubiKey.

Det starkaste försvaret mot nätfiske.

Senast i oktober 2017 lanserade Google sitt Advanced Protection Program (GAPP) för högrisk-användare som journalister, företagsledare och politiska kampanjteam. GAPP-programmet skärper ytterligare säkerheten för användare av Google-konton genom att kräva säkerhetsnycklar från hårdvarustyrda FIDO U2F för säker inloggning kontra optimal funktion. För att tillhandahålla det starkaste försvaret mot nätfiske går Advanced Protection bortom traditionell tvåstegsverifikation. Deltagare i GAPP måste logga in på ditt konto med ett lösenord och en fysisk säkerhetsnyckel, d.v.s. YubiKey. Andra verifieringsfaktorer, såsom koder som skickas via SMS eller Google Authenticator app, kommer inte längre att fungera, eftersom dessa former av 2FA har visat sig vara åtkomliga för nätfiske.

Skydda Adwords kunder

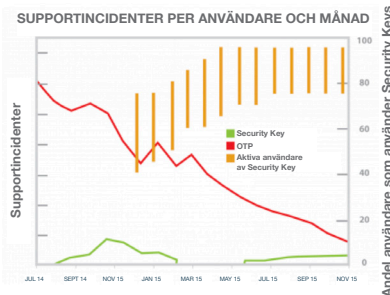
Google har också belyst fördelarna med att skydda Adwords-konton med YubiKey. 2016 publicerade Google en blogg som lyfte fram hur två digitala marknadsföringsbyråer, Jellyfish och iProspect, skyddar sina konton, kunder och inkomster genom att använda YubiKey.

Storskalig modern verifiering

Google är ett ledande teknologiföretag med innovation och uppfinningar som sin kärnverksamhet. I sitt samarbete med Yubico hade Google avgörande betydelse för definitionen av den öppna standarden för stark verifiering, numera känd som FIDO U2F-standard. Idag erbjuder Yubico och Google mer än en miljard Gmail-användare och mer än 50 000 Google-anställda stark resistens mot nätfiske genom verifiering med två faktorer för att därmed skydda personliga uppgifter och ge säker tillgång till internet. Säkerhetsnycklar har lett till [noll bekräftade kontointrång](#) och större användarnöjdhet efter storskalig spridning.

Mayank Upadhyay, direktör för säkerhetsutformning, Google Inc.

"Vi tror att vi genom att använda denna symbol har höjt säkerhetsstandarderna för våra anställda bortom vad som var kommersiellt möjligt. Enheten fungerar med Google's webbläsare Chrome, och arbetar väldigt smidigt för människor i deras dagliga arbetsflöde här på Google."



Om Yubico Yubico sätter nya globala standarder för enkel och säker tillgång till datorer, servrar och internetkonton. Yubico grundades 2007, är privatägt och har kontor i Australien, Tyskland, Singapore, Sverige, Storbritannien och USA. Ta reda på varför nio av de topp 10 internetmärkena och miljontals användare i mer än 160 länder använder vår teknologi på 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 USA
844-205-6787 (utan extra avgift)
650-285-0088