yubico

Pressmeddelande
01 juni 2026 23:00:00 CEST

Yubico samarbetar med OpenAI när passkeys blir ett krav för användare i Trusted Access for Cyber (TAC)-programmet

Passkeys lägger grunden för nätfiskeresistent autentisering och gör det möjligt för cybersäkerhetsteam och Codex-utvecklare att skydda de mest kraftfulla AI-modellerna och kodbaserna.

Yubico, ledande inom nätfiskegresistent autentisering och skaparen av YubiKey – den säkraste formen av hårdvarubaserad passkey – meddelar idag sin roll i att stärka säkerheten kring nästa generations AI-tjänster när OpenAI inför krav på passkeys för användare inom sitt program Trusted Access for Cyber (TAC).

Som ett ledande globalt företag inom AI-forskning och AI-utveckling sätter OpenAI en ny standard för hur användare kan ta kontroll över sin egen säkerhet med säkrare autentiseringsalternativ. Från och med den 1 juni 2026 kommer personer i TAC med tillgång till OpenAI:s mest kraftfulla AI-modeller med utökade behörigheter, att behöva aktivera Advanced Account Security (AAS). Kravet markerar en ny branschstandard: när man arbetar med AI-agenter, känsliga kodmiljöer och avancerade cybersäkerhetsfunktioner blir beprövade säkerhetslösningar som hårdvarubaserade passkeys inte längre ett val – utan en förutsättning.

”Vi lever i en tid där AI kan analysera sårbarheter och agera på våra vägnar. I den världen blir identiteten hos personen som kontrollerar AI den mest kritiska säkerhetsfaktorn”, säger Albert Biketi, produkt- och teknikchef på Yubico. ”OpenAI:s beslut är ett viktigt steg framåt för branschen. Det innebär en förflyttning från säkerhetslösningar som bygger på sannolikhet – där vi hoppas att ett lösenord är tillräckligt starkt – till kryptografiskt skydd som endast hårdvarubaserad autentisering kan erbjuda. Vi välkomnar OpenAI säkerhetsstrategi, där passkeys, exempelvis i form av en hårdvarubaserad säkerhetsnyckel, används för att ge de mest utsatta användarna ett starkare skydd.”

Därför spelar hårdvarubaserad säkerhet en viktig roll för AI: **Så ger Yubico OpenAI:s TAC-program en säker grund**
I takt med att AI utvecklas mot allt mer autonoma agenter, såsom Codex, blir utvecklarkonton och identiteter allt viktigare att skydda. Ett intrång kan i dag innebära obehörig åtkomst till kod, system och utvecklingsmiljöer. OpenAI nya krav möjliggör en modernare säkerhetsnivå genom:

- **Starkare skydd för TAC-användare:** Passkeys, inklusive hårdvarubaserade passkeys som YubiKeys, ger det nätfiskeresistenta skydd som krävs inom Advanced Account Security-programmet.
- **Attestering för företag:** Organisationer kan uppfylla OpenAI säkerhetskrav genom att integrera Yubicos nätfiskegresistenta autentisering i sina SSO-lösningar.
- **Säker återställning av konton:** I takt med att OpenAI avvecklar manuella kontoåterställningar hjälper Yubicos lösningar med primära och reservnycklar användare att behålla åtkomst till verksamhetskritiska system.

- **Verifiering av mänsklig avsikt:** Den fysiska beröringen av en YubiKey fungerar som en viktig kontrollmekanism som säkerställer att känsliga AI-relaterade åtgärder faktiskt godkänns av en verifierad användare.

Kravet bygger vidare på samarbetet mellan Yubico och OpenAI för att erbjuda hårdvarubaserad säkerhet till dem som utvecklar och använder framtidens AI-teknik. För mer information om hur Yubico hjälper organisationer att säkra AI-relaterade arbetsflöden, besök Yubicos webbplats.

För mer information kontakta:

Karin Muskopf
Global Communications
press@yubico.com

Om Yubico

Yubico (Nasdaq Stockholm: YUBICO), som utvecklat YubiKey, erbjuder högsta möjliga skydd för att stoppa så kallade nätfiskeattacker, på engelska kallat phishing-resistent multi-factor authentication (MFA), vilket gör inloggning enkel, säker och tillgänglig för alla. Sedan företaget grundades 2007 har det varit ledande när det gäller att sätta globala standarder för säker åtkomst till datorer, mobila enheter, servrar, webbläsare och internetkonton. Yubico är grundare och huvudsaklig bidragare till de öppna autentiseringsstandarderna FIDO2, WebAuthn och FIDO Universal 2nd Factor (U2F) och är en pionjär när det gäller att leverera hårdvarubaserad nyckel-autentisering i stor skala till kunder i över 175 länder.

Yubicos teknologi möjliggör inloggning utan lösenord tack vare den mest säkra formen av nyckelteknologi. YubiKeys fungerar direkt i över tusen konsument- och företagsapplikationer och tjänster och levererar hög säkerhet med en snabb och enkel upplevelse.

Som en del av missionen att göra internet säkrare för alla donerar Yubico YubiKeys till organisationer som hjälper högriskpersoner genom det filantropiska initiativet Secure it Forward. Företaget har sitt huvudkontor i Stockholm, Santa Clara och Singapore. För mer information om Yubico, besök oss på www.yubico.com.

Bifogade filer

Yubico samarbetar med OpenAI när passkeys blir ett krav för användare i Trusted Access for Cyber (TAC)-programmet