yubico

Nätfiskeskyddat MFA för dina hybrid- och distansarbetande medarbetare

Fem steg för att öka säkerheten och produktiviteten

Hybrid- och distansarbete är här för att stanna. En anpassning till ett flexibelt hybrid- och distansarbete kan samtidigt skapa IT-säkerhetsutmaningar, vilket gör det ännu viktigare att vara rörlig och acceptera den digitala omvandlingen. Med medarbetare som är geografiskt utspridda är befintliga typer av autentisering som traditionellt använts för platssäkerhet – som användarnamn och lösenord samt mobilbaserad autentisering – inte längre tillräckliga för att skydda åtkomsten till nätverk, applikationer och uppgifter. Det är enkelt att hacka användarnamn och lösenord och mobilbaserad autentisering är sårbar för nätfiske, skadlig kod, SIM-bedrägeri och man-in-the-middle-attacker, vilket gör att din organisation riskerar att drabbas av intrång.

Skydda dina hybrid- och distansarbetande medarbetare mot cyberhot med YubiKey – en hårdvarunyckel för flera protokoll från Yubico med tvåfaktorautentisering (2FA) som skyddar mot nätfiske, multifaktorautentisering (MFA) och lösenordsfri autentisering. YubiKey finns i flera olika formfaktorer och erbjuder en portabel och enkel användarupplevelse på alla stationära och bärbara datorer, mobila enheter och handdatorer. YubiKey möjliggör även lösenordsåterställning med självservice, vilket avsevärt minskar kostnaderna för IT-support. Organisationer runt om i världen använder YubiKeys för att säkerställa att de anställda har säker åtkomst till företagsnätverk, uppgifter och program, samt för att minska driftskostnaderna.

Ta hjälp av följande fem steg för att skydda dina medarbetare, ditt nätverk och dina enheter med YubiKey:

1 Aktivera MFA-åtkomst för system för identitets- och åtkomsthantering (Identity and Access Mangement) och identitetsleverantörer

De flesta ledande hybrid- och molnmiljöer använder sig av IAM-lösningar för att de anställda ska kunna arbeta utan att behöva krångla med flera användarnamn och lösenord för olika företagsapplikationer och -tjänster. Genom att aktivera multifaktorautentisering (MFA) på din IAM-plattform kommer din säkerhetsnivå att höjas.

Öka säkerheten i hela organisationen genom att aktivera multifaktorautentisering (MFA) med YubiKey. Ledande IAM-plattformar som Axiad, Duo, Google Cloud, Microsoft Azure Active Directory, Okta Workforce Identity, OneLogin, Ping Identity platform och RSA SecurID® har ett inbyggt stöd för YubiKeys, och kan användas för allt från Single Sign On (SSO) till meddelande- och videokonferensappar som Microsoft Teams, Google Hangouts och Zoom.

2 Eliminera beroendet av mobilbaserad autentisering för att skydda dig mot kontokapning

Tvåfaktorautentiseringsmetoder som engångslösenord och enhetsbaserade meddelanden är kopplade till mobila enheter, som kan infekteras av skadlig kod, SIM-bedrägeri och man-in-the-middle-attacker. Forskning av Google, NYU och UCSD baserad på 350 000 verkliga kapningsförsök har visat att SMS- och mobilautentiserare inte är särskilt effektiva som skydd mot kontoövertaganden och riktade attacker.[1]

YubiKey-integrationer som hjälper till att skydda dina hybrid- och

DUO FORGEROCK idaptive intercede Microsoft okta

ONE IDENTITY onelogin Onion ID PingIdentity secure W2

[1] Googles säkerhetsblogg: Ny forskning: Hur effektiv är den grundläggande kontohygienen när det gäller att förhindra kontoövertaganden

Skydda dina medarbetare mot kontokapning genom att byta ut befintlig mobilbaserad autentisering mot YubiKey. Genom att utnyttja moderna öppna autentiseringsstandarder som FIDO2 och WebAuthn kan du tillhandahålla säkerhetsgarantier på högsta nivå för att skydda dina medarbetare mot nätfiske- och man-in-the-middle-attacker.

3 Säker teknik för fjärråtkomst med MFA

För VPN-teknik (Virtual Private Networks) eller IAP (Identity-Aware Proxies) används av många olika organisationer för åtkomst till företagsnätverk, skyddade resurser eller specifika program. När en anslutning är etablerad är det säkert att ansluta via VPN eller IAP, men att ansluta från ett oskyddat hemnätverk eller ett publikt WiFi-nätverk kan vara riskabelt om autentiseringen förlitar sig på traditionella autentiseringsmetoder.

YubiKey säkerställer säker fjärråtkomst genom att möjliggöra nätfiskeskyddat 2FA eller MFA för ledande VPN-program som Pulse Secure och Cisco AnyConnect, samt annan programvara för fjärråtkomst, med hjälp av resurser som smartcard (PIV), engångslösenord (OTP), FIDO U2F eller FIDO2.

70%

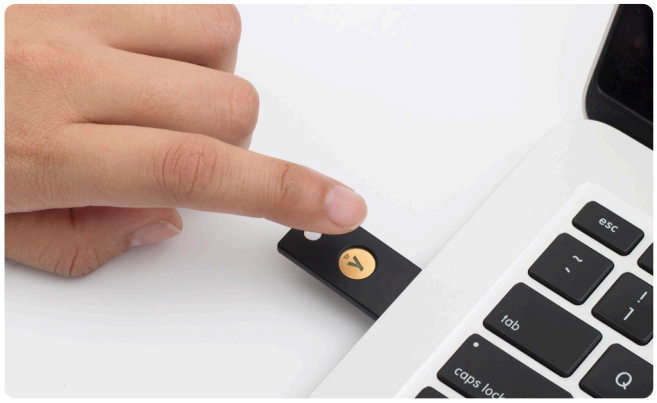
av anställda vill arbeta på distans eller i ett hybridupplägg.[2]

[2] Owl Labs: State of Remote Work Report 2021

4 Skydda datorinloggningarna med MFA

Många företagsanställda förlitar sig på lösenordshanterare, men om din lösenordshanterare inte är skyddad av nätfiskesäkrad MFA blir den sårbar för attacker och kan ge en angripare tillgång till din databas med lösenord för alla dina företagsapplikationer.

YubiKeys skyddar datorinloggningar, lokalt installerade program och kritiska affärsdata. De olika alternativen för multipel inloggning inkluderar autentisering för Mac:ar och Windowsdatorer inklusive sådana som är anslutna via Azure Active Directory, Active Directory och Microsoft Accounts. Ett av de mest effektiva sätten att säkra datoråtkomst är att använda YubiKeys smart card-funktionalitet, som kräver en YubiKey och en PIN-kod.



5 Kom igång redan idag och implementera YubiKeys sömlöst till din hybrid- och distanspersonal

Yubico erbjuder flexibla och kostnadseffektiva företagsplaner för organisationer med 500 användare eller fler att välja bort föråldrad MFA och anamma nätfiskesäkrad autentisering i stor skala.

Med en YubiEnterprise Subscription kan organisationer dra nytta av en förutsägbar OPEX-modell, flexibilitet att uppfylla användarpreferenser med valfria YubiKey-nycklar, uppgraderingar till de senaste YubiKey-nycklarna och snabbare driftsättning med enkel åtkomst till driftsättningstjänster och prioriterad support. Prenumerationskunder kan också köpa ytterligare tjänster och produkterbjudanden.

Kontakta Yubicos säljteam idag.

YubiKeys används i

9 av de 10 bästa internetteknikföretagen

4 av de 10 största Amerikanska bankerna

5 av de 10 största internationella detaljisterna

Om Yubico, uppfinnaren av YubiKey – Yubico gör säker inloggning till en enkel sak. Yubico är en ledande aktör när det kommer till internationella standarder för säker åtkomst till datorer och mobila enheter, och har även starkt bidragit till utformningen av de öppna autentiseringsstandarderna FIDO2, WebAuthn och FIDO Universal 2nd Factor (U2F). Besök: www.yubico.com för mer information.

Yubico AB
Kungsgatan 44
andra våningen
SE-111 35 Stockholm
Sverige

Yubico Inc.
5201 Great America Pkwy
Suite 122
Santa Clara, CA 95054
USA