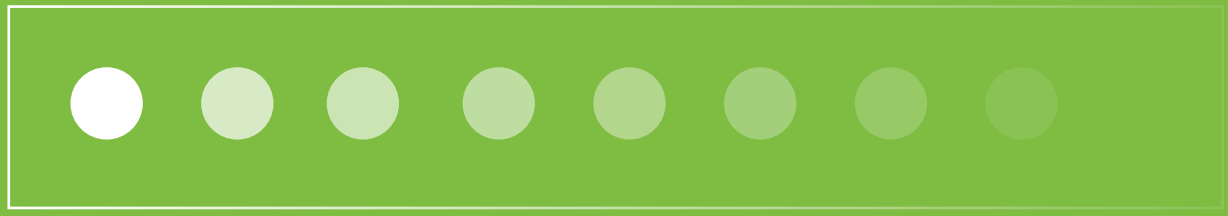
yubico

ETT WHITE PAPER FRÅN YUBICO
OKTOBER 2020

Going Passwordless

med FIDO2 och WebAuthn



Innehållsförteckning

Ledningens sammanfattning 3
Tid och kostnad för lösenord 4
Lös problemet med lösenord med FIDO2 6
Introduktion av lösenordslös autentisering 7
  FIDO2/WebAuthn autentiseringsval 8
Fördelar med att bli lösenordslös 9
  Förbättrad användbarhet 9
  Förbättrad säkerhet 10
  Förbättrad effektivitet 11
  Lika bekvämt som ett bankkort 12
  FIDO2, WebAuthn och FIDO U2F 13
Nya användarexempel med lösenordslös inloggning 14
  Anställda 14
  Detaljhandel 14
  Finans 15
  Tillverkning 15
  Hälso- och sjukvård 15
  Sälj- och leverantörsnätverk 16
Slutsats 17
Rekommendationer 18
Referenser 19

Ledningens sammanfattning

Föreställ dig en värld där användare inte längre behöver skapa, återställa, glömma och återigen återställa massor av lösenord. Lösenord är känt som den svagaste länken i affärssäkerhet och ett hinder för strömlinjeformade kundresor och interna processer. Världen håller på att förändras med introduktionen av lösenordslös autentisering. I en global undersökning av Ponemon Institute bland 2 507 IT-säkerhetsutövare och 563 enskilda användare upptäcktes att fyrtio-nio procent av IT-säkerhetsrespondenterna och 51 procent av individerna delar lösenord med kollegor för att komma åt företagskonton. Detta illustrerar de dåliga metoderna som förvärrar säkerhetsproblemen som lösenord kan skapa[1].

Den nya FIDO2/WebAuthn-autentiseringsstandarden erbjuder möjligheter för organisationer att lösa de problem som hör till lösenordsbaserad säkerhet. FIDO2 är en öppen standard, utvecklad i samarbete mellan Yubico, Microsoft och andra medlemmar av FIDO-alliansen. Den möjliggör utökade valmöjligheter för stark autentisering inklusive flexibiliteten att nu erbjuda lösenordslös, enkelfaktors- eller flerfaktors stark autentisering till användare och stöder dessutom det existerande scenariot med autentisering genom två faktorer.

Lösenordslös autentisering gör det möjligt att förvandla företagssäkerhet och användarupplevelse i varje bransch, såsom hälso- och sjukvård, tillverkning och detaljhandel, liksom för kontorspersonal, kompanjoner och leverantörer. Det kan förenkla för användaren att komma igång och mot bakgrund av att lösenord för närvarande står för den största av kostnaderna för IT-support så kan lösenordslös inloggning markant minska arbetsbelastningen på IT-callcenters, där personalen idag spenderar avsevärd tid med att skapa och återställa lösenord.

Hur kan kund- och arbetskraftsresor strömlinjeformas med lösenordslös inloggning? Vilka nya produkter och tjänster blir möjliga när lösenord inte längre behovs? Detta är frågor som framtidstänkande företags-och IT-ledare borde ställa sig nu.

Den här vitboken ger bakgrunden till lösenordslös autentisering och överväganden för företagsutveckling.

Tid och kostnad för lösenord

Företag letar idag efter olika sätt att dra nytta av molnet och mobil teknologi för att kunna leverera förbättrade produkter och tjänster snabbare och effektivare. Emellertid, företag som jagar ambitiösa planer för att strömlinjeforma kund- och arbetskraftsresor finner snart att de stöter på säkerhetsutmaningar.

Säkerhetsteknologi och kontroller införs för att skydda företaget, men just dessa säkerhetskontroller kan göra användare frustrerade. Högt på allas listor över ohanterliga, irriterande säkerhetskontroller står lösenord.

Lösenord har sedan 1950-talet varit en del av livet för företagsanvändare, liksom för konsumenter. Nästan varje digital upplevelse kräver dem - från sociala nätverk som Facebook till banker och detaljhandlare som H&M och Zara och även affärsapplikationer som Salesforce and Quickbooks Online.

Medelkonsumenten i USA försöker hålla ordning på över 70 lösenord, som de använder till alla sina webbsidor och tjänster[2], medan affärsanvändare beräknas vara ansvariga för att memorera och använda ett ännu större antal lösenord, så många som 191.[3] I takt med att millenniegenerationen börjar utgöra en växande del av arbetskraften minskar tålamodet för att memorera alla dessa hemligheter visar en IBM-studie. Millenniegenerationen är mer benägna att återanvända lösenord - de memorerar högst åtta - och gör därmed kompromisser med säkerheten till förmån för bekvämligheten.[4]

Lösenordströtthet leder till dataöverträdelser

Användare blir trötta på att skapa nya lösenord för olika tjänster och vara tvungna att ändra dem med några månaders mellanrum enligt säkerhetspolicyernas diktat. För att minska behovet av memorering börjar många användare efterhand lita på förenklade lösenord, vilka olyckligtvis är enkla att spräcka. Eller så återanvänder de lösenord på många olika sidor, där inbrott i en tjänst kan öppna dörren till många.

80% av hackningsrelaterade intrång omfattar fortfarande komprometterade och svaga kontouppgifter, enligt Verizon Data Breach Investigations Report (DBIR) 2019. NCSC 2019 UK Cyber Survey-säkerhetsanalys visade att 23,2 miljoner komprometterade konton över hela världen använde 123456 som lösenord.[6]

Glömda lösenord leder till höga supportkostnader

När användare glömmer sina lösenord slutar det ofta med att de ringer till help desks eller support centers, vilket upptar värdefull tid. Frågor om att återställa lösenord står för nästan 6 % av aktiviteten hos callcenters och kostar stora företag mellan 5 och 20 miljoner USD årligen.

80% av hackningsrelaterade överträdelser innebär fortfarande komprometterade och svaga kontouppgifter.[5]

Verizon dataöverträdelser
Undersökning av överträdelser

Eftersom företag fortsätter att lägga till fler affärsapplikationer i sina portföljer ökar kostnaden för lösenord bara. I själva verket ägnar företagen 30 till 60 procent av sina supportsamtal till återställningar av lösenord.

Microsofts IT-team bytte till lösenordsfri autentisering och nu loggar 90 procent av Microsofts anställda in utan att ange ett lösenord. Som ett resultat sjönk hårda och mjuka kostnader för att supporta lösenord med 87 procent. Eftersom företag fortsätter att lägga till fler affärsapplikationer i sina portföljer ökar kostnaden för lösenord bara. Faktum är att företag ägnar 30 till 60 procent av sina supportsamtal till lösenordsåterställningar.[7]

Nästfiskeattacker riktar in sig på identitetsstölder

Nätfiske fortsätter att vara ett massivt säkerhetsproblem när attackteknikerna fortsätter att utvecklas. Fejkade e-postmeddelanden som uppmanar användare att upprepa sina identitetsuppgifter kan användas för att samla ihop ett stort antal uppgifter som sedan används av kontotjuvar. Omkring 30 % av alla nätfiskemejl öppnas av sina mottagare och över 7 % av alla e-postmottagare övertalades att öppna en bilaga eller klicka på en länk, som ofta är en inloggningslänk. De flesta nätfiskeattackerna leder sedan till installation av sabotageprogram som fungerar som en hävstång till flera brott.[9] Även om användare skapar komplicerade lösenord kan hackare få tillgång till dem genom nätfiske och inbrott i användarkonton.

Stulna listor på identitetsuppgifter tillgängliga för försäljning

När hackare bryter sig in i en organisation och stjäl identiteter får de inte bara tillgång till den organisationens konton utan också konton hos andra organisationer där konsumenter har använt samma kombination av användarnamn och lösenord. När till exempel hackare år 2016 stal 1 miljard inloggningsidentiteter på Yahoo! fick de tillgång till alla andra tillgängliga konton med samma kombination av användarnamn och lösenord. Miljarder stulna identiteter finns tillgängliga för försäljning på Dark Web och cyberkriminella lanserar nu automatiserade inloggningsförsök med denna guldgruva av stulna lösenord. Idag är nio av tio inloggningsförsök på populära handels- och banksidor robotdrivna attacker.[9]

Så länge som affärsdriven IT måste lita på lösenord för identifiering så kommer kostsamma supportkrav, svag säkerhet och frustrerande kundupplevelser vara oundvikliga. Glömda och stulna lösenord försämrar kundupplevelser, minskar märkeslojalitet och bidrar till förlorade inkomster.

Lös problemet med lösenord med FIDO2

Föreställ dig att du kan erbjuda snabb, bekväm och säker service till alla typer av användare, kunder såväl som anställda, utan att kräva lösenord och utan att du behöver ådra dig den operativa overheadkostnaden som lösenordshantering utgör. Föreställ dig att kunder, kompanjoner och anställda på sina datorer och mobiltelefoner kan få omedelbar tillgång till innehåll och tjänster de vill nå utan att behöva trolla fram lösenord ur minnet eller ringa supporten för hjälp. Föreställ dig nya tjänster som kan möjliggöras om identifiering var ögonblicklig och enkel. Föreställ dig IT-organisationer som befriar sig själva från det dagliga gnetet med, och kostnaderna för, att hantera och återställa lösenord.

FIDO2 autentiseringsstandarden ger möjlighet till lösenordsfri autentisering.

Fördelarna med lösenordslös autentisering

Förbättrad användbarhet
Lösenordslös autentisering befriar användare från att behöva komma ihåg och skriva in lösenord.

Förbättrad säkerhet
Lösenordslös autentisering eliminerar säkerhetsrisker som hänger ihop med stulna lösenord och brutala attacker mot inloggningsskärmar.

Förbättrad effektivitet
Lösenordslös autentisering eliminerar behovet hos IT-avdelningar att hantera lösenord.

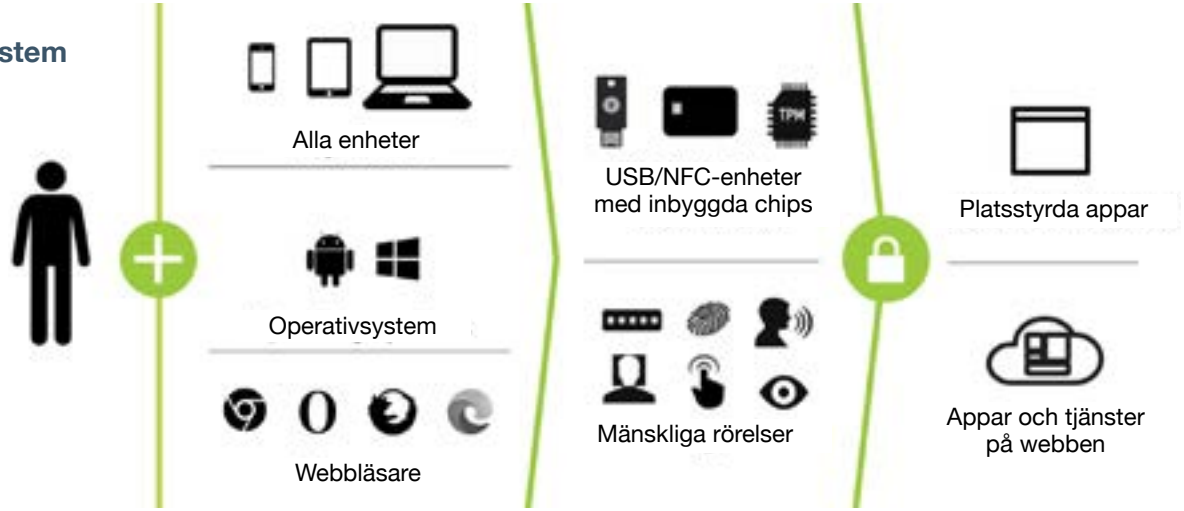
Dessa fördelar med lösenordslös autentisering kan nu nås med den, öppna autentiseringsstandarden FIDO2/WebAuthn.

Introduktion av lösenordslös autentisering

FIDO2 är en autentiseringsstandard som har tagits fram i samarbete mellan Yubico, Microsoft och medlemmar av FIDO Alliance, i kombination med World Wide Web Consortium (W3C), som stöder scenarier och upplevelser med flera användningsfall.

FIDO2 består av två standardiserade komponenter, en webb-API (WebAuthn) och en klient till autentiseringsprotokollet (CTAP). De två arbetar tillsammans och behövs för att åstadkomma en lösenordslös upplevelse vid inloggning. WebAuthn definierar en standardwebb-API som kan integreras i webbläsare och webbplattformars infrastrukturer för att ge användare metoder att säkert identifiera sig på nätet. CTAP gör det möjligt att en extern identifierare, som en säkerhetsnyckel, kan kommunicera starka autentiseringsidentiteter lokalt via USB, NFC eller Bluetooth till användarens PC eller mobiltelefon.

FIDO2 Ecosystem



FIDO2 är beroende av ett asymmetriskt par av krypteringsnycklar (offentliga/privata) för att autentisera användare. Den offentliga nyckeln kan sparas på alla tjänster eller datorenheter som stöds av FIDO2-autentisering, medan den privata nyckeln behålls hos användaren och skyddas på en fysisk säkerhetsnyckel som YubiKey5-serien och Security Key från Yubico. Autentiseringen i sig själv är snabb och enkel: genom att helt enkelt stoppa in eller knacka med säkerhetsnyckeln är autentiseringsutmaningen slutförd och inloggningen omedelbar.

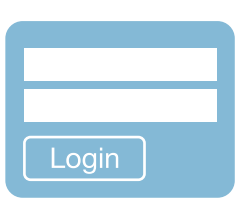
Med FIDO2 kan säkerhetsnyckeln användas för sig själv eller i kombination med en PIN eller gest för att åstadkomma lösenordslös autentisering. Dessutom fortsätter tvåfaktorsautentisering med lösenord att vara ett möjligt autentiseringssätt.

Stöd för FIDO2 från World Wide Web Consortium (W3C)

Webbverifieringens (WebAuthn) API-specifikation ger användare av webbläsare nya metoder att säkert identifiera sig på webben baserat på FIDO2-specifikationen. Webbläsarna Microsoft Edge, Google Chrome och Mozilla stöder alla WebAuthn API-specifikationen.

FIDO2/WebAuthn autentiseringsval

Enkelfaktor (lösenordslös)
Använd säkerhetsnyckeln för sig själv som en stark första faktor för autentisering. Du behöver bara ha en enhet som tillåter en knackning och du är på väg till din lösenordslösa upplevelse.



Två faktorer (Lösenord + identifikator)
Använd säkerhetsnyckeln som en andra faktor i en autentiseringslösning med två faktorer.

Flera faktorer (Lösenordslös + PIN eller biometri)
För att lösa högt ställda garantikrav: använd säkerhetsnyckeln för autentisering med flera faktorer, vilket kräver besittning av enheten, OCH en PIN-kod eller biometri.

FIDO2 stöds på den senaste versionen av Windows 10-enheter, inklusive Windows-stationära och mobila system. Detta gör FIDO2 tillgängligt på över 700 miljoner enheter runt om i världen och miljarder Azure AD-konton.

Fördelar med att bli lösenordslös

Förbättrad användbarhet

FIDO2 lösenordslös inloggning gör autentisering snabb och enkel genom att eliminera behovet av lösenord.

FIDO2 lösenordslös inloggning gör autentisering snabb och enkel genom att eliminera behovet av lösenord. Med FIDO2 kan en enskild hårdvaruidentifikator, som YubiKey, användas för att autentisera på alla tjänster en användare interagerar med, såsom affärsapplikationer och tjänster på jobbet, sociala medienätverk och andra konsumentapplikationer i hemmet - allt utan att dela några hemligheter.

Samtidigt kan FIDO2 användas för att stödja många olika identiteter för en enskild användare. Samma YubiKey kan användas för att få tillgång till såväl affärs- som konsumentapplikationer, webbsidor, tjänster, servrar och enheter - från byggnader till fordon - designade för att stödja FIDO2.

Med lösenordslös autentisering kan affärsfolk som reser med flygplan eller tunnelbanor som saknar Wi-Fi eller mobiluppkoppling fortfarande autentisera sina laptops och arbeta produktivt och säkert, även om deras brist på nätverk hindrar dem från att ta emot SMS eller OTP-identiteter för användarautentisering.

FIDO2 eliminerar behovet av nätverkstillgång (antingen mobil- eller internetbaserad) för att ta emot sekundära faktorer. Förutom att stärka IT-säkerheten gör FIDO2 det lättare för användare att nå de enheterde behöver för att arbeta närsomhelst, varsomhelst.

FIDO2 stöds på den senaste versionen av Windows 10-enheter, inklusive Windows-stationära och mobila system. Windows 10 har mer än 1 miljard användare världen över vilket gör cirka 700 miljoner enheter FIDO2-kompatibla.[10]

Eftersom FIDO2 har utvecklats som en öppen branschstandard och är brett uppbackad av Microsoft och World Wide Web Consortium (WC3) med stöd från Google och Mozilla, så är ett införande inte beroende av någon enskild existens. FIDO2 besparar företag kostnaden för investera i utveckling och underhåll av sedvanliga säkerhetsmodeller med avseende på problem med lösenord. Nu kan företag i alla branscher dra fördel av en öppen branschstandard för autentisering som rekommenderas av branschledare.

Vi uppfyller NIST standarder för autentisering

FIDO2 kan vara antingen ett enfaktors krypteringstecken eller ett flerfaktors krypteringstecken. Enligt specialpublikationen 800-63 från NIST är krypteringstecknet med flera faktorer kategoriserat som autentiseringsgaranti på nivå 3, vilket är den högsta garantinivån som deklarerats enligt denna standard. Användning av FIDO2 med en PIN uppfyller därför de högsta autentiseringskraven på reglerade marknader där överensstämmelse med NIST SP800-63 är obligatorisk.[11]

Förbättrad säkerhet

FIDO2 förbättrar dramatiskt säkerheten i användaridentifiering och tillgångshantering.

FIDO2 förbättrar dramatiskt säkerheten i användaridentifiering och tillgångshantering.

Med lösenordslös inloggning kan användare inte luras till att plötsligt avslöja lösenord, eftersom lösenord inte längre behövs. Användare identifierar sig med en hårdvaruidentifikator som YubiKey, vilken övergripande förklarat fungerar så här:

- YubiKey skapar och hanterar FIDO2-identiteten (ett offentligt/privat nyckelpar) samt knyter identitetn till den specifika tjänsten, känd som originalet. Originalbindning hindrar attacker på vägen.
- När den privata nyckeln fått ett identifieringsuppdrag av en tjänst som Azure AD används den till att signera svaret som sänds över nätverket och autentiseras av den onlinetjänst som använder den offentliga nyckeln.

FIDO2-identiteten, som lagras på ett säkert chip i YubiKey-nyckeln och som aldrig lämnar enheten, designas för att hindra hackare från att lura användare att logga in på sidor.

FIDO2 minskar risken för applikationer webbsidor, servrar och enheter genom att ta bort den centraliserade lagringen och hanteringen av känsliga identiteter. FIDO2-konton behöver inga lösenord; därför finns det inte längre en skatt av lösenord att stjäla. Webbsidor och andra tjänster lagrar bara offentliga nycklar som användare har registrerat, alltså bevaras hemligheten (den privata nyckeln) säkert på hårdvaruidentifikatorn och skickas aldrig över nätverket som ett traditionellt lösenord. Dessa offentliga nycklar kan godkänna signaturer som genererats av privata nycklar, men de kan inte användas på egen hand för att initiera tillgång till andra resurser. Endast en slutanvändare med den privata FIDO2-nyckeln kan framgångsrikt autentisera sig till en tjänst. Säkerheten förbättras medan också tillgången till inloggning blir snabbare, enklare och mer pålitlig för slutanvändare.

Autentiseringsprivilegier kan beviljas i enlighet med policyer som är specifika för organisationen eller nödvändiga enligt branschregler, såsom GLBA och HIPAA, eller regeringsföreskrifter som NIST SP800-63. Genom att rätta sig efter NIST SP800-63 garanterar FIDO2 överensstämmelse med ett brett spektrum av andra regelverk som bygger på NIST-standarder. IT-adminstratörer och tjänstemän kan lita på att användare inte kringgår autentiseringskontroller genom att dela lösenord på post-it-lappar eller via e-post. Varje användare får en unik nyckel som autentiserar dem till registrerade tjänster och applikationer.

“FIDO2 kräver inte någon komplex PKI-miljö för att hantera certifikat.”

Förbättrad effektivitet

FIDO2 gör det möjligt för IT-avdelningar - inklusive service desks och callcenters - att slippa skapa, lagra, cirkulera och återställa lösenord.

Lösenordslös inloggning ger möjlighet till krångelfritt mottagande av anställda och entreprenörer genom att eliminera supportkostnaderna för att ge ut och hantera lösenord. Istället för att ge nyanställda och entreprenörer temporära lösenord som måste ändras direkt och sedan ändras igen enligt ett fastställt schema, så ger FIDO2-autentisering möjligheten att helt enkelt utfärda en FIDO2 säkerhetsnyckel till varje användare och användaren anger ett valfritt PIN vid utfärdandet. Privilegier i samband med FIDO2-autentisering kan enkelt återkallas när en anställd eller entreprenör avslutar sina tjänster för företaget.

Genom att använda FIDO 2 säkerhetsnyckel kan användare identifiera sig själva till en central tjänst som Azure AD och etablera sina identiteter så att det kan registrera nya enheter, som exempelvis smartphones. I organisationer där datorenheter delas kan varje användare snabbt och enkelt autentisera utan att behöva komma ihåg och skriva in lösenord. Genom att helt enkelt sätta in eller knacka på en NFC-godkänd YubiKey kan användare låsa upp sina enheter och få tillgång till sina konton.

Dessutom kräver inte FIDO2 någon komplex PKI-miljö för att hantera certifikat. IT-avdelningar kan styra om sin tid och kraft till mer strategiska och produktiva uppgifter.

Uppfyller företagskrav för användarautentisering

FIDO2 uppfyller alla dessa kritiska krav för användarautentisering:

- **Erbjuder identiteter som inte kan bli hackade eller lurade**
- **Erbjuder en autentiseringsmetod som hindrar nätfiske**
- **Erbjuder bättre upplevelse för slutanvändare än lösenord**
- **Erbjuder maskinbunden autentisering och auktorisering - autentiseringen kan inte flyttas mellan maskiner**
- **Stöder varierande styrkor på autentisering**
- **Stöder mångfaldiga identiteter**
- **Kräver bara en enda användargest som en knackning eller ett drag med fingret för att godkänna tillgång**

Enkel inloggning ökar användandet av digitala tjänster med 10-20 %

Källa: McKinsey ClickFox survey[13]

Lika bekvämt som ett bankkort

För att uppskatta bekvämligheten med lösenordslös inloggning med hjälp av YubiKey, fundera på bekvämligheten med ditt bankkort. Du har förmodligen ditt bankkort med dig överallt. Du skyddar det; du låter det inte bara ligga där alla kan se det. För att låsa upp det i en ATM skriver du in en kort PIN-kod. PIN-koden ändras väldigt sällan om ens någon gång, du behöver inte komma ihåg något lösenord och inget användarnamn och ändå är till tillgången till bankomat väldigt säker.

En lösenordslös YubiKey är likartad. Du bär den med dig överallt. För att låsa upp en enhet - antingen en laptop dator, en smartphone, ett kontrollsystem för tillverkning, en hälso - och sjukvårdsportal eller någon annan enhet - så sätter du helt enkelt in din YubiKey i en USB-port eller placerar den nära en NFC-sensor. Sen, när du uppmanas till det, knappar du in en valfri PIN eller använder biometrisk kontroll, beroende på applikationen eller tjänsten.

Liksom PIN-koden på ditt bankkort ansvarar FIDO2 PIN för din tillgång till mekanismen bakom säkerhetsnyckeln. PIN-koden låser upp din FIDO2 säkerhetsnyckel och aktiverar ett nyckelbyte med vad som helst som den autentiserar mot: den lokala enheten, en avlägsen katalogtjänst, en webbsida, ett socialt nätverk eller någon annan IT-tjänst.

I vissa fall kan tjänster konfigureras att autentisera användare utan att kräva PIN-koder eller gester. Till exempel, för att erbjuda den snabbaste möjliga service till kunder kan en kompanjon till en detaljförsäljare få tillåtelse att autentisera sig bara genom att lägga sin nyckel på en NFC-platta som omedelbart låser upp ett datorsystem. Om datorsystemet är konfigurerat med en platta som upptäcker användarens närvaro kan systemet automatiskt logga ut användaren ur systemet när den autentiserade försäljningskompanjonen ger sig av.[12] Eftersom FIDO2 radikalt förändrar processen att autentisera användare kan företag rimligen ha råd med sina ytterligare autentiseringsåtgärder, eftersom användarupplevelserna av FIDO2 är så enkla och snabba och förbättrar produktiviteten och samtidigt minskar supportkostnaderna.

I alla dessa scenarier erbjuder FIDO2 lösenordslös inloggning en upplevelse som är snabbare och säkrare än användarnamn och lösenord. Lösenordslös inloggning förvandlar användarupplevelsen av att logga in på applikationer, webbsidor, tjänster, servrar och enheter till den välkända, sekundsnabba bekvämligheten i att komma in på en bankomat.

FIDO2 lösenordslös inloggning kräver användning av en FIDO2-certifierad identifikator, som YubiKey 5-serien.

FIDO2, WebAuthn och FIDO U2F

Hur fungerar FIDO2 och WebAuthn med FIDO U2F?

U2F är en öppen autentiseringsstandard som tillåter hårdvaruidentifikatorer, mobiltelefoner och andra enheter att säkert nå hur många webbaserade tjänster som helst - ögonblickligen och utan behov av drivrutiner eller särskild mjukvara. U2F skapades i samarbete mellan Google och Yubico, med bidrag från NXP, och förvaltas idag av branschkonsortiet för öppen autentisering, FIDO Alliance.

U2F är en stark autentiseringslösning, men det är en tvåfaktorslösning, som är beroende av användarnamn och lösenord som den första faktorn. 2F i namnet syftar helt enkelt på 2:a faktorn.

FIDO2 är en andra generation av U2F. FIDO 2 bygger på U2F genom att lägga till de beståndsdelar som krävs för att en användare ska kunna bli identifierad och autentiserad utan något lösenord. FIDO2-autentisering stöder enfaktors-, tvåfaktors- och flerfaktorsautentisering.

WebAuthn-komponenten i FIDO2 är bakåt kompatibel med FIDO U2F-autentiseringar. Det betyder att alla tidigare certifierade FIDO U2F säkerhetsnycklar inklusive YubiKeys, kommer att fortsätta fungera som en inloggningsupplevelse med andrafaktors autentisering med webbläsare och onlinetjänster som stöder WebAuthn.

Nya användarexempel med lösenordslös inloggning

Anställda

När nya anställda ska tas emot behöver företag inte längre utfärda tillfälliga lösenord eller lösenord av något slag. Istället kan de helt enkelt utfärda en hårdvara för autentisering, som YubiKey. Med hjälp av YubiKey kan en användare autentisera sig mot Azure AD eller andra tjänster med eller utan en kort PIN-kod, beroende på applikationen. YubiKey kan också användas för att registrera ytterligare enheter, som smartphones eller bärbara datorer, för att också fungera som autentiserare.

Autentiseringsprocessen kan bli anmärkningsvärt snabb och enkel. Till exempel, istället för att sitta ner och skriva in ett användarnamn och ett lösenord kan en kontorstjänsteman helt enkelt sätta sig, knacka med sin YubiKey och börja arbetsdagen.

Detaljhandel

Delägare, gruppledare, teamledare, kassörer och andra detaljhandelsanställda behöver snabb, enkel tillgång till IT-system. Lösenordslös inloggning effektiviserar mottagande och tillgång genom att tillhandahålla rigorös autentisering som en vakt mot bedrägeri.

Detaljhandlare har ofta säsongsanställda. Till exempel anställer en välkänd nordamerikansk detaljhandelskedja normalt 30 000 tillfälliga arbetare under semestersäsongen. Traditionellt sett skulle alla dessa arbetare ha behövt användarnamn och lösenord. Med FIDO2 kan de helt enkelt få säkerhetsnycklar utfärdade. Auktoriserade tjänster kan avaktiveras centralt genom en katalogtjänst som Azure AD när de säsongsbundna aktiviteterna avslutas.

FIDO2 besparar IT-avdelningen problemen med att skapa, återställa och återkalla lösenord. Om personal återanställs kan deras säkerhetsnycklar helt enkelt återaktiveras och delas ut igen för tillgång till butikstjänster.

Finans

Att göra snabb, krångelfri lösenordslös autentisering tillgänglig förbättrar märkesupplevelse, effektiviserar näthandel och interaktion inom kundsupport och stöder till och med skapandet av nya produkter och tjänster. En bank, kreditsammanslutning eller någon annan finansiell institution som erbjuder säkerhetsnycklar och lösenordslös autentisering till kunder minskar risken för kontointrång och förenklar samtidigt livet för sina kontoinnehavare.

Tillverkning

Liksom detaljhandlare har tillverkare många olika skift av arbetare. FIDO2 förenklar hanteringen av tillgång för denna ständigt föränderliga arbetsstyrka. Eftersom arbetare inte behöver skriva in lösenord men ändå kan identifiera sig själva unikt så effektiviserar FIDO2 tillgången till IT-system och stöder samtidigt intern säkerhet och policyer för identitetshantering. Samtidigt eliminerar det risken för att policyer för lösenordshantering (som exempelvis periodisk lösenordscirkulering) ska orsaka förseningar eller problem i verksamheten.

USA:s departement för nationell säkerhet har varnat för att tillverkningsindustrin fortfarande är ett utsatt mål för nätfiskeattacker, delvis eftersom hackare är intresserade av att stjäla intellektuell egendom.[14] Genom att ersätta lösenord som kan kapas av nätfiskare med FIDO2 säkerhetsnycklar kan tillverkare hjälpa till att stänga dörren för den här sortens attacker, tack vare stark autentisering som ger försvar mot nätfiske.

Hälso- och sjukvård

Hälso- och sjukvårdsorganisationer (HCOs) är känsliga för dataintrång av olika slag. Information om patienthälsa, som patienthistoria och betalningsinformation, är tio gånger mer värdefull på den svarta marknaden är kredikortsdata.[15] Varför? Därför att medicinskt bedrägeri, som insamling av falska försäkringsfordringar, betalar sig.

Hälso- och sjukvårdsorganisationer är också känsliga för attacker med krav på lösensummor, av vilka många lanseras genom nätfiske. Genom att ersätta lösenord med säkerhetsnycklar, kan hälso- och sjukvårdsorganisationer och deras affärspartners i hög grad minska sin sårbarhet för den här typen av attacker.

FIDO2 kan också hjälpa hälso- och sjukvårdsorganisationer att försäkra sig om att information om personlig hälsa (PHI) kan nås enbart av behöriga användare i enlighet med regleringen i HIPAA. En nyligen genomförd branschundersökning visade att 73% av läkarna i USA har kommit åt information om personlig hälsa genom att använda en kollegas lösenord.[16] Att förenkla inloggningsprocesser uppmuntrar läkare att använda enbart sina egna identiteter för att komma åt patientinformation och annan skyddad data och tjänster och sluta att dela identitetshandlingar med varandra. I vilket fall som helst begränsar det dem till att dela tillgång endast med människor som är fysiskt närvarande. Däremot kan delade lösenord tillåta tillgång från vilken plats som helst.

FIDO2 tillhandahåller en annan viktig fördel för hälso- och sjukvårdsbranschen: snabb, enkel autentisering. Läkare och sjuksköterskor måste logga in dussintals gånger om dagen medan de flyttar från patient till patient, från rum till rum och från enhet till enhet. Nu kan tillgången bli ögonblicklig och säkrare med lösenordslös inloggning. Vårdgivare kan fokusera på att ge vård istället för att fumla med krångliga inloggningsprocedurer.

Sälj- och leverantörsnätverk

Antalet dataintrång relaterade till tredjepartsleverantörer har ökat med 22% sedan 2015.[17]

Att stärka partnerportalens autentisering med FIDO2 säkerhetsnycklar effektiviserar tillgången för partners och eliminerar samtidigt möjligheten att lösenord används för att infiltrera i ett företag genom dess partnerportal.

Dessutom kräver inte FIDO2 någon affärsverksamhet för att hantera alla sina leverantörers identiteter. Istället kan en affärsverksamhet helt enkelt anta en "inga lösenords"-policy och kräva att säljare autentiserar sig genom att använda en säkerhetsnyckel. Säljare kan enkelt skaffa FIDO2 säkerhetsnycklar på egen hand. Den här sortens sammanslutning var tidigare inte möjlig med andra autentiseringsteknologier, vilka gjorde det alltför kostnadskrävande att säkra säljarnätverk.

Slutsats

Lösenord har hämmat användare, säkerhetsteam och IT-team för länge. Genom att möjliggöra lösenordslös säkerhet öppnar FIDO2 en ny era inom företags-IT, kundservice och interaktion mellan människa och maskin.

Genom att använda lösenordslös inloggning kan företag stärka nätverkssäkerheten, minska IT-kostnader, förbättra produktiviteten, och skapa en ny klass av lönsamma tjänster som möjliggörs av snabbt, bekvämt och allmänt utbrett förtroende. Lösenordslösa inloggningserbjudanden:

- **Förbättrad användbarhet** Med lösenordslös inloggning behöver användare aldrig pausa för att skriva in lösenord och kämpa med att komma ihåg dem. Tillgången blir snabb och enkel.
- **Förbättrad säkerhet** Att ta bort lösenorden eliminerar säkerhetssvagheter som beror på stulna lösenord, lösenord som stulits genom nätfiske och brutala kraftattacker mot enkla lösenord.
- **Förbättrad effektivitet** En lösenordslös värld befriar IT-administratörer från ombesörjandet av tio- eller hundratusentals lösenord. IT-support-lasten minskar, fastän säkerhet och användbarhet samtidigt förbättras.

FIDO2 är en lösning som nu är tillgänglig för hundratals miljoner Windows 10-enheter med en uppgradering till den senaste versionen av Windows 10. Det är en lösning som IT-säljare och IT-avdelningar på företag kan börja arbeta med för att möta inte bara interna IT-säkerhetsbehov, utan också kundernas.

Hur kan kundresor effektiviseras med lösenordslös inloggning? Hur kan användarupplevelser föreställas på nytt sätt utan behovet av lösenord? Hur skulle det vara om tillgången till applikationer och tjänster kunde vara snabb, enkel och säker överallt?

Vilka nya produkter och tjänster blir möjliga när lösenord inte längre behovs, när avlägsna laptops och mobila enheter enkelt kan spridas och bli pålitliga och när risker för dataintrång och bedrägeri - på lång sikt - avsevärt minskar?

Detta är de frågor som framtidsorienterade företags- och IT-ledare borde ställa sig nu.

FIDO2 lösenordslös inloggning gör att dessa frågor inte är spekulativa frågor för futurister, utan snarare en praktisk fråga - även en överhängande fråga - för CISO:s, produktchefer, marknadsförare och andra som är engagerade i att leverera bästa möjliga produkter, tjänster och upplevelser och samtidigt försäkra sig om att autentiseringen alltid är säker.

Rekommendationer

Hur bör företagsledare, CIO:s, CTO:s och andra IT-ledare förbereda sig för en lösenordslös värld? Yubico erbjuder följande rekommendationer:

Håll dig informerad

Prenumerera på uppdateringar från Yubico genom att besöka www.yubico.com/go-passwordless

Gå med i Yubicos program för utvecklare

Utvecklare bör gå med i Yubico Developer Program för att få tillgång till workshops, fri mjukvara och utvecklingsstöd.

Uppgradera alternativ för autentisering med två faktorer idag

Inkludera support för FIDO2 säkerhetsnycklar och var redo att ta dig till lösenordslös inloggning.

Utveckla en strategi för att bli lösenordslös

Samla ihop ett team av affärs- och IT-ledare inom din organisation för att överväga hur ni kan dra maximal nytta av lösenordslös autentisering. Till att börja med kan teamet vilja:

- Utveckla en kostnadsmodell för lösenord. Hur många help desk och callcenter-frågor är knutna till lösenord? Hur lång tid tar en typisk fråga? Hur lång tid tar det för administratörer att dela ut lösenord till nya användare? Hur mycket produktivitet förloras på grund av utestängning från konton? Mät tid och kostnader för era nuvarande autentiseringsmetoder så ni kan förstå kostnadsbesparingarna.
- Identifiera pilotprojekt som kan låta ditt team rulla ut lösenordslös inloggning till en utvald användargrupp. Fokusera på områden som kräver stark autentisering där det skulle medföra stora fördelar att optimera användarupplevelsen. Övervaka utrullningens förlopp och applicera alla lärdomar på framtida utrullningar.

Referenser

1. ”2020 State of Password and Authentication Security Behaviors Report”. Ponemon Institute. https://pages.yubico.com/2020-password-and-authentication-report
2. “New Research: Most People Have 70-80 Passwords”. Newswire. https://www.newswire.com/news/new-research-most-people-have-70-80-passwords-21103705
3. “Average Business User Has 191 Passwords”. Security Magazine. https://www.securitymagazine.com/articles/88475-average-business-user-has-191-passwords
4. Kessem, Limor. “Millennial Habits May Bring An End To The Password Era | SC Media”. SC Media. https://www.scmagazine.com/millennialhabits-may-bring-an-end-to-the-password-era/article/746144/
5. “Data Breach Investigation Report”. Verizon Enterprise. https://enterprise.verizon.com/resources/reports/dbir/2019/introduction/
6. “Most hacked passwords revealed as UK cyber survey exposes gaps in online security”. National Cyber Security Center, 2019 Cyber Security Survey. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security
7. “Protect your accounts with smarter ways to sign in on World Passwordless Day”. Microsoft. https://www.microsoft.com/security/blog/2020/05/07/protect-accounts-smarter-ways-sign-in-world-passwordless-day/
8. Verizon, ibid.
9. Ward, Kelsey. “Credential stuffing rules the day as 90% of login attempts no longer made by humans”. Secureidnews.com. https://www.secureidnews.com/news-item/credential-stuffing-rules-the-day-as-90-of-login-attempts-no-longer-made-by-humans/
10. “Statistic: the total market share of Windows 10 version 1903/1909 edition reach 75.2%”. Meterpreter. https://meterpreter.org/statistic-the-total-market-share-of-windows-10-version-1903-1909-edition-reach-75-2/
11. “NIST SP 800-63 Digital Identity Guidelines”. Nist.Gov. https://www.nist.gov/itl/tig/projects/special-publication-800-63
12. “Pcprox® Mat | RF Ideas”. Rfideas.Com. https://www.rfideas.com/products/presence-detectors/pcprox-mat
13. “Is Cybersecurity Incompatible With Digital Convenience?” McKinsey & Company. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/is-cybersecurity-incompatible-with-digital-convenience
14. “Energy Sector Tops List Of US Industries Under Cyber Attack, Says Homeland Security Report - Iot Now - How To Run An Iot Enabled Business”. Iot Now - How To Run An Iot Enabled Business. https://www.iot-now.com/2015/03/12/30962-energy-sector-stays-top-of-the-list-ofus-industries-under-cyber-attack-says-homeland-security-report
15. “Your Medical Record Is Worth More To Hackers Than Your Credit Card”. Reuters. https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924
16. “Survey Reveals Sharing EHR Passwords is Commonplace”. HIPAA Journal. https://www.hipaajournal.com/sharing-ehr-passwords-commonplace/
17. “Data trust pacesetters show how to create and protect value from data”. PwC. https://www.pwc.com/us/en/services/consulting/cybersecurity/data-trust-pacesetters.html

yubico

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