okta

Wat is de prijs van identity-diefstal?

Onze persoonsgegevens zijn waardevol voor criminelen. En dat is te merken aan de explosieve stijging van het aantal account takeovers, waarbij hackers zich met authentieke inloggegevens toegang tot accounts verschaffen om informatie te stelen. De impact op de omzet en de reputatie van een organisatie kan enorm zijn. Maar hoe kunnen organisaties de risico's beperken en digital trust opbouwen?

Account takeovers zijn aan de orde van de dag

Het aantal account takeovers is tijdens de pandemie verdrievoudigd omdat meer mensen online gingen winkelen en werken.

3x

Stijging tussen 2019 en 2021

Bron: Sift

Identities van gebruikers liggen onder vuur

Gestolen of gehackte inloggegevens zijn de belangrijkste oorzaak van alle datalekken in 2021.

61%

van de datalekken in 2021 is terug te voeren op misbruik van inloggegevens

Bron: Verizon DBIR

> “Hackers breken niet in, ze loggen in"
>
> Bret Arsenault, Microsoft

Inloggegevens worden op meerdere manieren buitgemaakt

Criminelen voeren phishingaanvallen uit om gebruikers inloggegevens te ontfutselen of kopen lijsten met veelvoorkomende en gestolen wachtwoorden op het dark web.

7 op de 10

organisaties zien een toename van phishingaanvallen sinds het begin van de pandemie.

Bron: Sophos

15 miljard

inloggegevens worden openlijk te koop aangeboden op het dark web

Bron: Dark Shadows

Zwakke wachtwoorden wakkeren het probleem aan

Veel mensen gebruiken makkelijk te raden wachtwoorden of hetzelfde wachtwoord op meerdere websites, waardoor het risico op een aanval nog groter wordt.

123456

Meest voorkomende wachtwoord in 2021

Bron: NordPass

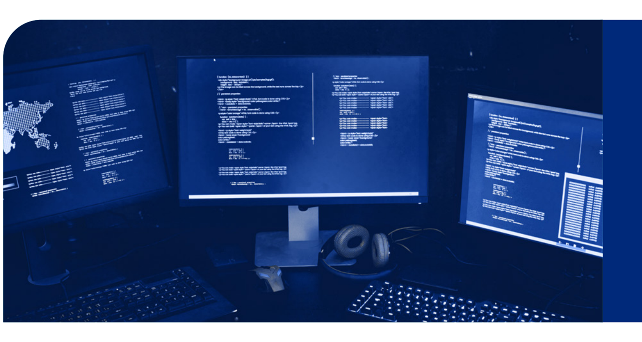
14

Gemiddeld aantal keren dat hetzelfde wachtwoord wordt gebruikt

Bron: LastPass

Hoe dringen hackers uw systemen binnen?

Credential stuffing	Password spraying	Phishing
Hackers testen gestolen inloggegevens op duizenden verschillende websites totdat het lukt om toegang tot een account te krijgen. Dit werkt vaak omdat veel mensen steeds dezelfde inloggegevens gebruiken.	Hackers overspoelen gebruikersaccounts met veelgebruikte wachtwoorden om te zien of er eentje tussen zit dat werkt. Dit lukt vaak omdat veel mensen eenvoudig te raden wachtwoorden gebruiken.	Hackers proberen gebruikers inloggegevens te ontfutselen, bijvoorbeeld via een e-mail waarin de gebruiker wordt gevraagd op een link naar een website te klikken.



55%

van de datalekken wordt uitgevoerd door georganiseerde criminele groepen

Bron: Verizon DBIR

Datalekken zijn slecht voor uw organisatie

Veel cybercriminelen gebruiken online tools om massa's verschillende wachtwoorden op websites af te vuren tot ze een ingang hebben gevonden.

47%

van de klanten laat een merk voorgoed links liggen als ze horen dat er een datalek is geweest

Bron: The State of Digital Trust, Okta

$ 4,2 miljoen

Gemiddelde kosten van een datalek in 2021

Bron: : IBM Cost of a Data Breach Report

Drie manieren om identities van klanten te beschermen

1. Detecteer lekken sneller

Detectiesystemen, zoals Credential Guard van Auth0, kunnen inbreuken detecteren op het moment dat die zich voordoen en vervolgens snel de betreffende wachtwoorden resetten.

2. Implementeer multi-factor authenticatie

Multi-factor authenticatie voegt een extra beveiligingslaag toe aan het wachtwoord van een gebruiker om hackers uit uw systemen te weren.

3. Passwordless experience

Steeds meer organisaties kiezen ervoor om helemaal geen wachtwoorden meer te gebruiken en in plaats daarvan klanten veilige, gebruiksvriendelijke inlogmethoden te bieden, zoals biometrie, eenmalige wachtwoorden en magic links.

Voorkom account takeovers met Okta

Okta beschermt uw klanten, partners en werknemers met authenticatie-oplossingen die ze kunnen vertrouwen. Zo kunt u sterke password policies hanteren, frauduleuze inlogpogingen snel opsporen en kwaadwillenden blokkeren met Okta's geautomatiseerde dreigingsdetectie.

Als u meer wilt weten over het stoppen van account takeovers, bekijk dan de videopodcast met Brian Glick, hoofdredacteur van Computer Weekly, en Ian Lowe van Okta.