CLOUDFLARE

솔루션 요약

강력한 인증으로 피싱 공격을 막는 방법

보안 키와 Zero Trust 접근법은 피싱 공격자를 막을 수 있습니다

피싱에 의한 위협

데이터 손실, 네트워크 손상, 계정 도난

오늘날 조직이 겪는 가장 큰 위협 요소 중 하나는 특정 목표를 겨냥한 피싱 공격입니다. 피싱과 소셜 엔지니어링 공격은 사람을 조종하여 중요한 정보나 액세스를 얻는 것이 목적입니다. 일반적으로 로그인 자격 증명을 대상으로 삼습니다.

이런 종류의 공격이 성공하면 다음과 같은 결과를 초래할 수 있습니다.

- 계정 탈취
- 더 규모가 큰 공급망을 공격할 연결고리가 생김
- PII 및 IP 등 데이터 유출
- 랜섬웨어 등 맬웨어 공격

다행히, 매우 효과적인 솔루션이 있어 피싱 위험을 줄일 수 있습니다. 가장 중요한 솔루션 하나는 다단계 인증(MFA)입니다.

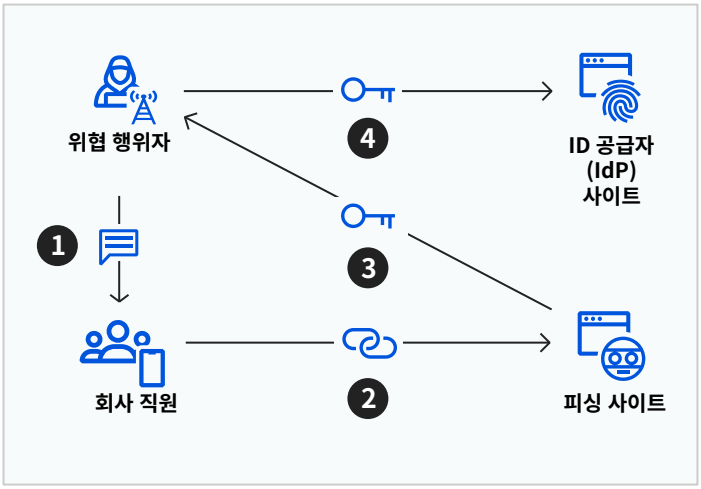


그림 1: SMS 피싱 공격의 구조. 1. 정상적으로 보이는 문자 메시지를 전송합니다. 2. 정상적으로 보이는 사이트와 연결되어 있습니다. 3. 피해자의 자격 증명과 시간 기반 일회용 비밀번호가 실시간으로 전달됩니다. 4. 실제 회사의 IdP 사이트에 로그인합니다.

다단계 인증(MFA)으로 피싱 공격을 막는 방법

MFA는 비밀번호 도난을 무력화시킵니다

MFA에서 사용자는 로그인 시 사용자 이름 및 비밀번호와 함께 키를 입력해야 합니다. 사용자에게 이 키가 없으면 계정에 액세스할 수 없으며, 공격자도 마찬가지입니다.

소프트 키를 사용하는 MFA

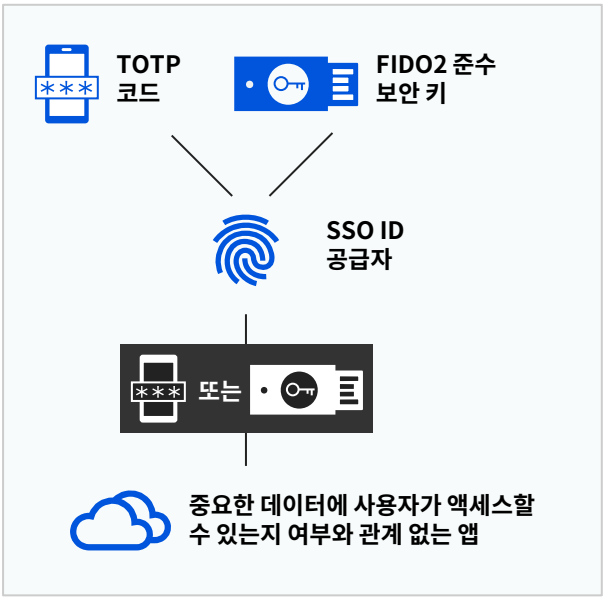
일반적으로 MFA를 구현할 때는 시간 기반 일회용 비밀번호(TOTP)와 같은 소프트 키를 사용합니다. TOTP는 보통 SMS 메시지, 이메일이나 앱으로 발급됩니다. 단일 단계 인증보다 안전하긴 하지만 공격자가 소프트 키를 가로챌 수도 있습니다.

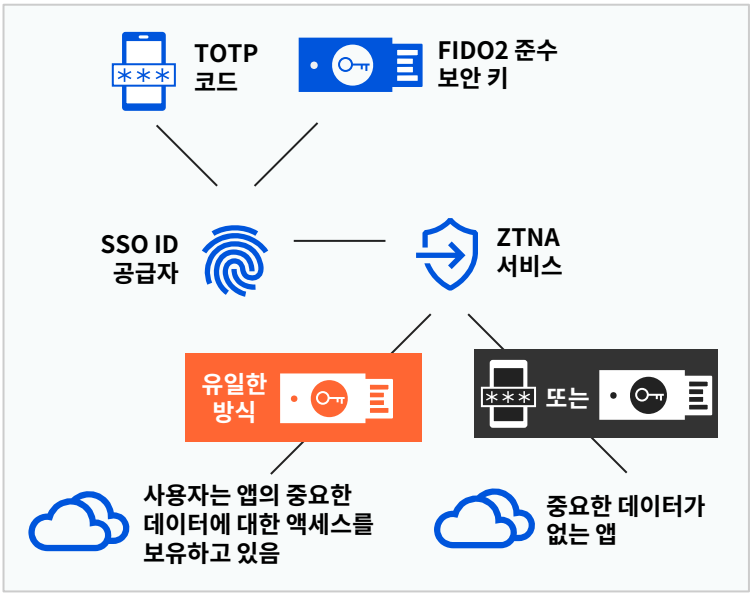
보안 키를 사용하는 MFA

FIDO2 준수 보안 키가 발급된 다음에는 공격자가 가로챌 수 없습니다. 물리적으로 접근하지 않는 한 거의 훔칠 수 없습니다. Google 연구에 따르면 FIDO2/U2F 준수 보안 키를 사용하자 계정 탈취 시도가 100% 차단되었습니다.[1]

선별적으로 강력한 인증 시행

일부 IAM 솔루션에서 강력한 인증을 지원할 수도 있지만, 관리자가 이를 실제로 요청할 수는 없을 가능성도 있습니다. ZTNA를 사용하면 특히 중요한 데이터를 보관하는 앱에 FIDO2 인증을 필수로 시행할 수 있게 됩니다. Cloudflare는 모든 인증 시 보안 키 MFA를 요구합니다. 이런 방법으로 Cloudflare의 보안 상태를 크게 강화했습니다.

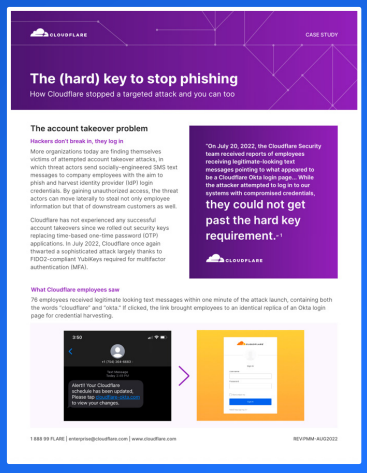




"2022년 7월 20일에 Cloudflare 보안팀은 Cloudflare Okta 로그인 페이지로 보이는 사이트와 연결된 정상적으로 보이는 문자 메시지를 받고 있다는 소식을 직원들한테 들었습니다... 공격자는 손상된 자격 증명으로 당사 시스템에 로그인하려고 했지만,

하드 키를 요구하는 단계를 통과할 수 없었습니다." [2]

CLOUDFLARE



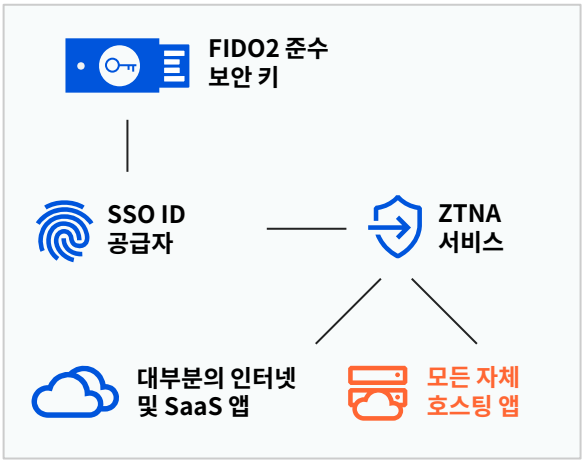
강력한 인증을 모든 곳에 도입하세요

모든 앱에 적용되는 FIDO2 준수 MFA

기존의 다양한 방법으로 특히 SSO(Single Sign On) 서비스를 사용하는 클라우드 서비스에 MFA를 시행할 수 있습니다. 그러나 이러한 인증 유형을 기본적으로 지원하지 않는 레거시 또는 비 웹 앱의 경우 이러한 방식으로 시행하기는 어려울 수 있습니다.

ZTNA 롤아웃 단순화

Zero Trust 네트워크 액세스(ZTNA)는 모든 리소스에서 집계 계층 역할을 수행하며, 각 리소스에 인증 정책을 엄격하게 적용합니다. SaaS, 자체 호스팅, 비 웹 애플리케이션은 모두 ZTNA의 보호를 받을 수 있습니다. 이를 통해 모든 애플리케이션에 걸쳐 강력한 인증을 더욱 쉽게 시행할 수 있습니다.



강력한 인증을 구현하려는 조직에 대한 핵심 사항

1

IAM 중앙화

MFA를 모든 앱에 걸쳐 더 쉽게 구현할 수 있도록 ID 및 액세스 관리(IAM)를 중앙화하세요.

2

선별적으로 MFA 시행

ID와 컨텍스트에 따라 선별적으로 MFA 옵션(TOTP 및 FIDO2 또는 FIDO2만)을 시행하세요.

3

모바일 장치 지원

노트북, 데스크톱 컴퓨터, 서버, 모바일 장치에 FIDO2 솔루션을 마련하세요.

1. krebsonsecurity.com/2018/07/google-security-keys-neutralized-employee-phishing/
2. Cloudflare 블로그 게시물, 2022년 8월 9일, "지능적 피싱 사기의 원리와 Cloudflare에서 공격을 차단한 방법", blog.cloudflare.com/2022-07-sms-phishing-attacks/