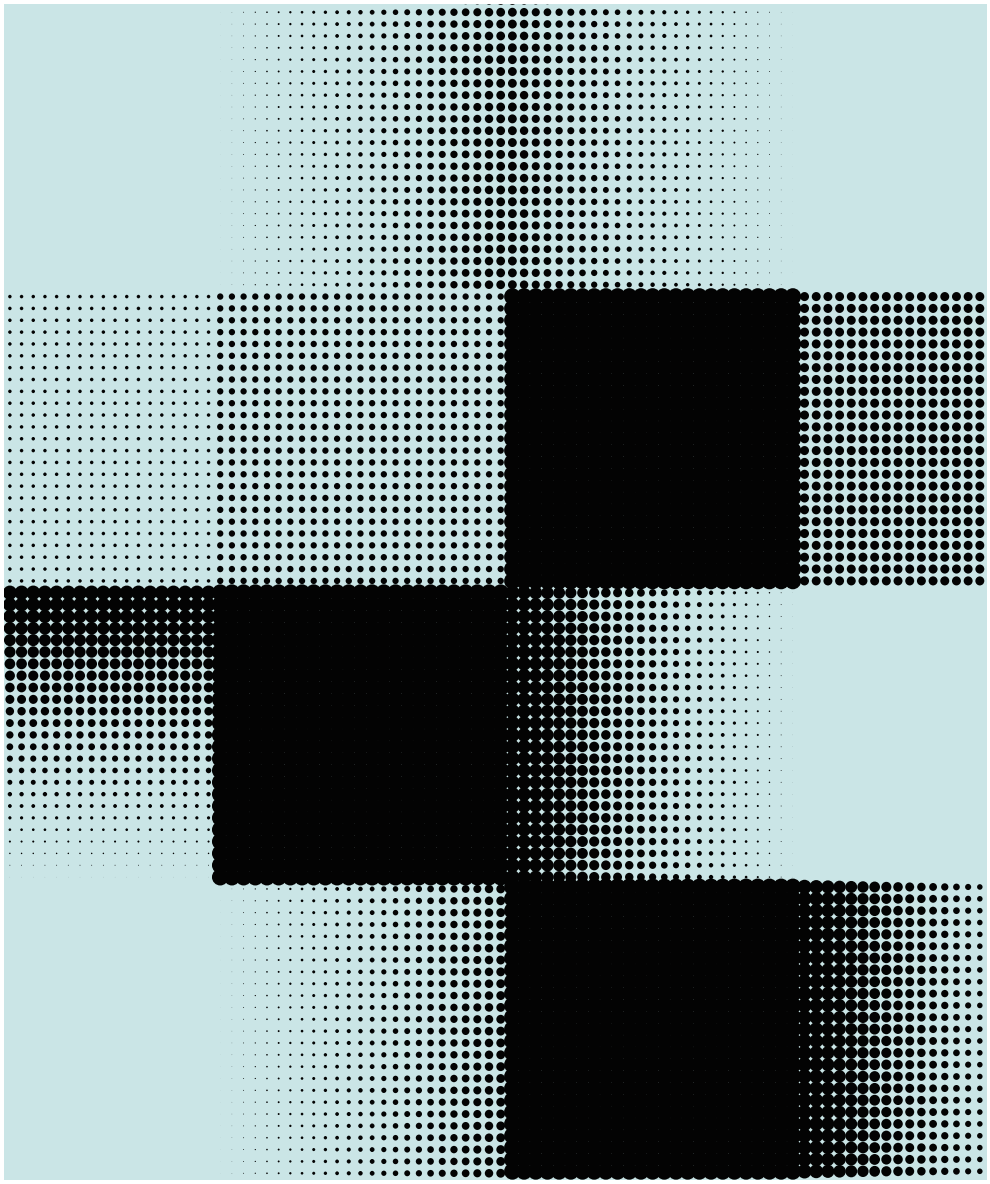
백서

2020년 11월

다중 요소 인증 개발 가이드

MFA 솔루션 선정 및 MFA 배포 계획을 위한 완벽 가이드

Okta Inc.
서울 강남구 테헤란로 152
강남파이낸스센터 41층
support.okta.com
050-6626-1877



okta

목차

서론

최근 몇 년간 비밀번호에 대한 보안 위협이 증가면서 소비자를 비롯한 기업 웹 및 모바일 애플리케이션에서 안심하고 인증을 보호할 수 있는 방법으로 다중 요소 인증(MFA)이 빠르게 도입되고 있습니다.

일반적으로 인증은 알고 있는 요소(비밀번호 등), 보유하고 있는 요소(ID 카드 등), 생체 요소(지문 등)의 세 가지 요소 중 하나를 검증하여 이루어집니다. 다중 요소 인증에는 두 가지 이상의 요소가 사용됩니다.

웹 제품이나 모바일 제품은 대체로 비밀번호와 함께 사용자가 보유하고 있는 시간 기반 토큰, 모바일 앱에 대한 푸시 알림 또는 생체 인식을 사용하여 다중 요소 인증을 도입하는 경우가 많습니다. 하지만 MFA에 대한 접근 방식은 차이가 크기 때문에 절충 효과도 각기 다릅니다.

본 가이드에서는 MFA 솔루션 도입을 쉽게 결정할 수 있는 이유와 MFA 배포 모범 사례를 정리했습니다. 또한 IDG와 함께 실시한 설문조사 결과를 검토하여 업계의 우선순위가 무엇인지, IAM(Identity and Access Management)이 강력한 인증과 보안을 구현하는 데 어떤 역할을 하는지 알아봅니다. 그런 다음 정책이나 액세스 요건 등 MFA 솔루션을 배포하기 전에 고려할 사항에 대해 살펴봅니다. 마지막으로 지금까지 엔지니어링 팀이나 제품 팀과 함께 협력하면서 쌓아온 노하우를 바탕으로 애플리케이션용 MFA 솔루션을 개발하는 사람들에게 실질적으로 도움이 될 만한 정보를 제공합니다.

대규모 데이터 유출 시대에 필요한 IAM과 MFA

오늘날 악성 코드, 해킹, 피싱, 사회 공학 등 다양한 위협 요소가 넘쳐나면서 이러한 공격 전략이 계정 침해나 자격증명 도용으로 이어지고 있습니다.

아이덴티티와 관련하여 가장 우려되는 보안 문제

59%

직원 외 사용자 추가에 따른 사용자 기반 확장

43%

불편한 인증 제어 환경 무시/와해

33%

IAM 정책의 부재

29%

동일 비밀번호 재사용

24%

탈취된 자격증명

가장 시급한 아이덴티티 및 액세스 관리 과제

61% 애플리케이션 환경의 아이덴티티 및 액세스 관리

35% 현재 사용되는 보안 솔루션 통합(규모가 큰 기업의 경우 50%)

35% 사용자 액세스 정보와 패턴을 수집하여 보고할 수 있는 능력

향후 전망 - IAM 우선순위 결정 및 현재 IAM 테크놀로지에 대한 평가

92%

77%
관리자

30%
자격증명 침해를 탐지할 수 있는 능력이 양호하거나 우수하다고 보고

45%
IAM 데이터를 보안 운영 센터(SOC)와 통합

보안 문제 해결: IAM 솔루션에서 가장 중요한 잠재적 이점


모든 앱과 서비스에 대한 인증을 통해 사용자 기반을 안전하게 확장 — 53%


프로비저닝/디프로비저닝의 자동화 — 45%


사용자 제어에 따른 불편을 줄여 사용자 경험을 개선 — 43%


보다 엄격한 액세스 제어 도입 — 43%

* IDG 연구 조사 발췌

다중 요소 인증(MFA)을 사용하기 전에 고려해야 할 8가지 사항

비밀번호는 관리하기 쉽지 않습니다. 비밀번호를 안전하게 보호하기 위해 보안 요건이 나날이 증가하고 있지만, 여기에는 부정적인 영향도 있습니다. 보안 요건에 맞게 비밀번호를 복잡하게 만들더라도 기억하기가 힘들기 때문에 결국 같은 비밀번호를 여러 사이트에서 재사용하게 됩니다. 개중에는 메모지에 대충 적어 놓고 사용하는 사람들도 있습니다. 반려 동물의 이름이나 생일, 전화번호와 같이 쉽게 알아낼 수 있는 글자나 숫자를 조합하기도 합니다. 하지만 이는 데이터를 안전하게 보호하는 방법이 아닙니다.

다행스러운 점은 해커에게는 어려우면서도 적법한 사용자에게는 쉽도록 액세스를 구현해야 한다는 점을 기업들이 인식하고 이를 위한 조치를 단행하고 있다는 사실입니다. 이러한 개념을 가장 효과적으로 실현할 수 있는 방법이 바로 다중 요소 인증, 즉 MFA입니다. MFA는 사용자의 앱과 서비스를 무단 액세스로부터 안전하게 보호할 수 있는 방법입니다. MFA 배포를 계획할 때 고려해야 할 몇 가지 사항을 소개합니다.

1. 사용자 교육

조직은 비밀번호만 사용하는 액세스 환경에서 보안 위험을 줄이기 위해 MFA를 배포하지만 이를 불편하게 여기는 사용자들도 있습니다. 이러한 프로세스 변경으로 인해 귀중한 시간을 허비하게 될까 봐 걱정이 앞설 수 있습니다. 결국 일회용 비밀번호(OTP)를 입력하거나, 혹은 푸시 알림을 수신하느라 로그인 절차에 소요되는 시간이 늘어나게 되기 때문입니다. 그럼에도 불구하고 우리는 경영진에서부터 IT 팀, 보안 팀, 그리고 엔드 유저에 이르기까지 모두가 MFA로 전환하는 것에 동의하도록 만들어야 합니다. 모두가 자신의 역할을 다하여 회사를 안전하게 보호할 수 있도록 전 직원에게서 동의를 얻어야 합니다. 교육을 통해 이들의 동의를 얻을 수 있습니다. 각 사용자가 추가 인증 단계를 거침으로써 보안상의 어떤 이점을 얻을 수 있는지 이해시켜야 합니다. IT 팀에서 예정된 변경 사항을 사전에 알리기 위해 이메일을 발송하는 것도 흔히 사용되는 방식입니다. 이때 스크린샷과 FAQ, 그리고 지원 팀의 연락처 정보를 반드시 추가해야 합니다.

2. MFA 정책 고려

MFA를 배포할 때는 보안과 사용 편의성을 적절히 조율하여 한쪽으로 치우치는 것을 방지하는 것이 좋습니다. 따라서 MFA 정책을 정의할 때는 2차 요소의 사용 방식과 사용 시기를 고려해야 합니다. 언뜻 납득이 안 될 수도 있지만, 때로는 단계별 인증을 늘리기보다는 인증 횟수를 줄이는 게 더 효과적인 경우도 있습니다. 위험을 기반으로 효과적인 정책을 구성하여 필요할 때만 단계별 인증을 요구해야 합니다. 가령, 알려진 네트워크에서 로그인하는 경우 8시간마다 2차 인증 요소를 요구하거나, 혹은 새로운 디바이스나 장소에서 로그인하는 경우에만 2차 요소를 요구하는 정책도 가능합니다. 또한 중요한 데이터에 광범위하게 액세스하는 사용자 계정 그룹이 있다면 이들에게는 더욱 엄격한 정책을 적용해야 합니다. 예를 들어 소스 코드에 액세스하는 회사 소속 개발자나 중요한 데이터에 액세스하는 임원에게는 중요한 앱에 로그인할 때 더욱 강력한 유형의 요소를 입력하도록 하거나, 중요한 앱에 로그인 할 때는 MFA 프롬프트에 추가로 응답하도록 요구해야 합니다. MFA를 사용하면 이러한 사용자 그룹이 회사 이벤트 일정이 아닌 중요한 리소스에 액세스를 시도할 때 2차 인증 요소를 요구할 수 있습니다. MFA의 기본 개념은 보안을 저해하지 않으면서 우수한 사용자 경험을 구축할 수 있도록 추가 검증 절차를 사용자에게 최대한 투명하게 구축하는 것입니다.

3. 다양한 액세스 요건에 따른 계획 및 제공

사용자가 인터넷 연결은 가능하지만 휴대전화 통신사의 서비스는 거의 혹은 전혀 이용하지 못하는 경우가 있습니다. 와이파이가 제공되는 항공기, 교외 주택 또는 대형 콘크리트 건물의 지하실 등이 여기에 해당합니다. 이러한 상황에서는 음성이나 SMS를 사용하지 못하기 때문에 휴대전화의 인터넷 연결을 통해 통신이 암호화되는 푸시 또는 OTP 기반의 Okta Verify가 더 나은 선택이 될 수 있습니다. 이벤트 기반 또는 시간 기반의 일회성 비밀번호(TOTP)를 생성하는 하드웨어 디바이스에서는 통신 채널이 전혀 필요하지 않습니다. 조작이나 복제도 더욱 어렵습니다. 하지만 물리적 디바이스는 배포 비용 외에도 직원이 가지고 다녀야 하거나, 집에 놓고 오거나, 혹은 분실할 염려가 있습니다. 따라서 이러한 유형의 요소는 단기 계약자 또는 작업자가 자주 바뀌는 상황에서는 적합한 옵션이 될 수 없습니다. MFA 요소 측면에서는 광범위한 시나리오를 해결할 수 있는 옵션들이 많이 있습니다. 자사의 조직에서 각 시나리오에 가장 적합한 옵션을 선택하십시오. 모든 상황을 한 번에 해결할 수 있는 범용 솔루션이 없다면 여러 가지 정책과 요소를 사용하면 됩니다.

일반적으로 다음과 같은 배포 팁은 보안을 강화하는 동시에 엔드 유저 경험까지 개선하는 효과가 있습니다.

- MFA를 지원하는 하드웨어가 있다면 사용자가 생체 인식을 2차 요소로 사용할 수 있도록 허용하십시오(Windows Hello, Touch ID 등). 이렇게 하면 엔드 유저 경험을 간소화할 뿐만 아니라 사용자가 인터넷에 연결되지 못하는 상황까지 해결할 수 있습니다.
- 사용자가 두 가지 이상의 요소를 사용하여 한 가지는 백업용으로 남겨놓을 수 있도록 허용하십시오.
- 사용자가 인증 요소를 직접 리셋할 수 있도록 허용하십시오(분실한 휴대전화의 인증 프로그램 앱 리셋 등).
- 강력한 요소 유형(모바일 앱 인증 프로그램, 푸시 알림, 생체 인식)을 활성화한 경우에만 배포를 시작하십시오.

4. SMS를 사용하는 OPT에 대한 재고

SMS는 사용자에게 익숙하며 롤아웃하기 쉽습니다. 휴대전화와 태블릿이 급속히 확산되어 거의 모두 가지고 있다 보니 SMS는 OTP 전송 시 공통적으로 사용되는 통신 채널이 되었습니다. SMS는 일반적으로 이러한 목적으로 사용하기에 충분히 안전하다고 여겨집니다. 여기에는 인프라가 매우 전속적이고 불투명하다는 사실도 하나의 이유입니다. 조사 결과에 따르면 SMS는 보안이 부족하며, 이미 알려진 취약점에 대해서만 보안이 제공된다고 합니다. SMS를 사용할 때는 이동통신 사업자의 보안에 의지할 수밖에 없습니다. 하지만 이동통신 사업자에게 보안 모범 사례가 구축되어 있다고 신뢰하더라도 스푸핑이나 사회 공학을 통한 침해 위험은 늘 도사리고 있습니다. 대부분 경우 공격자가 자신이 제어하는 디바이스로 사용자의 전화번호를 복사하여 SMS 메시지와 OTP에 액세스하는 것은 기술적으로 그리 어렵지 않기 때문입니다.

SMS OTP를 MFA 요소로 사용할 때 흔히 발생하는 문제

1. 개인 계정의 비밀번호를 비즈니스 계정에서도 재사용하는 직원들

   휴대전화에 내장된 SIM 카드에는 이용 중인 모바일 사업자와 통화 대상에 관한 정보가 저장됩니다. SIM 스왑/SIM 해킹 공격에서는 위협 행위자가 사용자를 사칭하여 사업자를 속입니다. 결국 사용자의 전화번호가 다른 휴대전화의 SIM 카드에 할당됩니다.

   SIM 스왑/SIM 해킹 공격은 수년간 문제로 지적되어 왔지만 2019년에 발생한 사건으로 대중들에게 널리 알려졌습니다. **Twitter CEO인 잭 도시(Jack Dorsey)의 Twitter 계정이 위협 행위자들의 공격을 받아 모바일 사업자가 잭의 전화번호를 위협 행위자들이 소유한 휴대전화로 전환한 것입니다.** SIM 스왑/SIM 해킹 공격에서는 위협 행위자가 계정에 액세스하기 위해 물리적 디바이스에 액세스할 필요가 없습니다. 전화번호가 위협 행위자들이 소유한 디바이스로 전환되면 사용자의 온라인 계정에 연결된 SMS OPT 메시지를 모두 수신할 수 있기 때문입니다.

2. 분실된 디바이스와 동기화된 디바이스

   휴대전화를 분실하면 매우 짜증이 나겠지만 실제로 간혹 발생하는 일입니다. 그런데 전화번호가 금융 앱이나 소셜 미디어 등에 연결되어 있다면 어떻게 될까요? 일반적으로 다중 요소 인증은 자신의 신원을 입증할 수 있는 두 가지 요소를 조합한 것으로 알려져 있습니다. 여기에는 지식적 요소(알고 있는 정보), 선천적 요소(생체 인식 정보) 또는 소유적 요소(가지고 있는 정보)가 포함됩니다. 비밀번호와 SMS OTP를 요소로 사용한다면 지식적 요소와 소유적 요소가 결합된 경우에 해당합니다. 하지만 휴대전화를 분실했다면, 이론적으로는 아이덴티티를 검증할 수 있는 메시지를 더는 수신할 수 없게 됩니다. 그렇더라도 다수의 디바이스에서 메시지를 동기화할 수 있기 때문에 2차 요소라고 할 수 있는 디바이스를 분실하더라도 계정에 액세스하는 데 아무런 문제가 없습니다. 다만 비밀번호가 포함되어 있을 수 있는 텍스트 메시지를 이메일로 전송하거나, 혹은 PIN 코드 유무에 관계없이 어떤 디바이스에서든 액세스할 수 있는 VoIP 번호를 사용한다면 이 방법도 안전하지 않습니다.

3. 온라인 모바일 계정 탈취

   일반적인 모바일 사업자들은 웹 포털에서 온라인 계정을 통해 텍스트 메시지를 확인할 수 있도록 허용하고 있습니다. 웹 포털 계정이 2차 요소로 보호되지 않거나, 여러 온라인 계정에서 쉽게 추측할 수 있는 비밀번호를 사용한다면 위협 행위자가 계정을 모니터링하여 금융 앱, Facebook 등을 초기화할 때 받았던 SMS OTP 메시지를 찾아 해당 계정에 액세스할 수 있습니다.

4. 사회 공학 및 피싱

유감스럽게도, 사회 공학적 피싱 공격에 취약한 인증 방식은 SMS OTP뿐만이 아닙니다. 비밀번호나 보안 질문과 같이 비교적 안전성이 떨어지는 요소들도 피싱 공격에 취약합니다. 사회 공학 공격에서는 위협 행위자가 사용자가 신뢰하는 서비스의 직원을 사칭하여 계정 자격증명을 넘기도록 유도합니다. 이때 대체로 SMS OTP도 디바이스로 전송됩니다. 가령, “은행”에서 보안 문제로 인해 사용자 계정에 당장 액세스해야 한다는 전화를 받는다면 자신도 모르게 위협 행위자에게 사용자 이름과 비밀번호, 그리고 로그인 과정에서 휴대전화로 전송되는 SMS OTP 코드까지 알려주는 실수를 저지를 수 있습니다. 피싱 공격은 이메일을 통해서만 일어나는 것이 아닙니다. 텍스트 메시지 형태로도 전송됩니다. 게다가 악성 웹사이트인지 모른 채 자신의 사용자 이름과 비밀번호를 무심코 입력하게 되면 위협 행위자가 앞서 언급했던 공격 유형을 이용해 계정을 탈취할 수 있습니다.

NIST는 이러한 이유로 SMS를 사용할 때 위험에 대비하라고 권장하지만 근본적으로 사용자, 사용 사례, 그리고 보호할 데이터에 따라 사용자가 위험을 스스로 평가해야 합니다. 결국 SMS에 MFA를 사용하는 것이 전혀 사용하지 않는 것보다 안전합니다.

5. 신중한 규정 준수 요건 확인

PCI DSS, SOX, HIPAA 등 대부분의 IT 규정 준수 표준들은 강력한 사용자 인증 제어를 요구하기 때문에 MFA 배포를 위한 동기 부여가 될 수 있습니다. 뻔한 얘기 같지만 이러한 표준을 따르는 것이 목표라면 요구사항을 상세히 알아보고 거기에 맞춰 구성과 정책을 조정해야 합니다. 일례로 PCI 표준과 HIPAA 표준의 경우 강력한 인증, 즉 알고 있는 정보, 보유하고 있는 정보, 생체 인식 정보의 세 가지 요소 중 적어도 두 가지 이상을 사용하는 인증 방법을 요합니다. SOX는 테크놀로지에 두는 비중이 적지만 감사를 통과하려면 기업의 재무 데이터와 회계 데이터가 안전하다는 것을 입증해야 합니다. IT 규정을 따르려면 관련 표준을 이행해야 하지만 표준을 충족했다는 사실도 입증할 수 있어야 합니다. 따라서 감사를 통해 표준을 충족한다는 사실을 빠르고 확실하게 입증하려면 구성 및 이행 과정에 문서화 단계를 추가해야 합니다. 이로써 미래의 자신과 자신의 회사가 성공을 거둘 수 있습니다.

6. 분실한 디바이스에 대한 계획 수립

일반적으로 MFA를 배포할 때는 2차 인증 요소로 “가지고 있는 정보”가 사용됩니다(1차는 “알고 있는 정보”, 3차는 “생체 인식 정보”). 예를 들어 SMS나 음성, 혹은 Okta Verify나 Google Authenticator와 같은 인증 앱의 경우에는 사용자가 휴대전화를 가지고 있습니다. YubiKey나 RSA 등의 하드웨어 토큰의 경우에는 사용자가 토큰을 가지고 있습니다. 하지만 사용자가 가지고 있다면 분실할 가능성도 있습니다. 따라서 분실한 디바이스에 대한 처리 절차가 포괄적 IT 지원 플레이북에 포함되어 있어야 합니다. 처리 범위를 확대하여 MFA에 사용되는 디바이스까지 추가하고 디바이스 분실이 보고되면 다음과 같은 처리 절차로 이어져야 합니다.

- 현재 세션 종료 및 사용자 재인증 요청
- 사용자의 계정 및 액세스 권한에서 해당 디바이스 연결 해제
- 모바일 디바이스에 저장된 기업 정보 원격 삭제(필요한 경우 일반적으로 회사 소유 디바이스에서 실행)

또한 디바이스가 분실되었을 때 일정 기간 이전에 사용자 계정 활동에 대한 감사를 통해 비정상적인 활동의 유무를 살피는 것도 중요합니다. 이때 의심스러운 활동이 발견되면 데이터 유출 가능성을 고려하여 상급자에게 보고해야 합니다. 당면한 보안 문제를 처리했다면 이제 해당 직원이 업무에 복귀할 수 있도록 대체 가능한 디바이스 또는 로그인 방법을 제공해야 합니다. 예를 들어 IT 지원 부서에 전화하여 아이덴티티 요건을 확인하는 등의 대체 프로세스를 통해 대체 요인이 실행되는 동안 직원이 생산성을 유지할 수 있습니다.

7. 원격 근무자에 대한 MFA 배포 계획 수립

원격 근무가 증가하고 있기 때문에 기업은 이에 맞춰 보안을 강화해야 합니다. 이상적인 보안 환경이라면 입사자 계정을 회사에서 관리하고, 기존 직원들은 IT 시스템에 직접 액세스할 수 있어야 합니다. 하지만 원격 근무의 확산으로 인해 배포와 문제 해결 측면에서 새로운 과제가 나타나고 있습니다. 배포 관련 문제를 해결하려면 사용자가 빠르게 정상적으로 구성할 수 있는 요소를 사용하는 것이 가장 좋은데, 예를 들면 내장형 디바이스 생체 인식이나 Okta Verify와 같은 모바일 앱 인증 프로그램이 있습니다.

이러한 방식으로 사용자는 하드 토큰이 추가로 제공될 때까지 기다릴 필요가 없습니다. 이는 엔드 유저 커뮤니케이션이 중요한 경우에도 마찬가지인데, 설정 및 문제 해결에 필요한 리소스를 얻을 수 있기 때문입니다. 입사자 계정 관리의 경우에도 일부 기업은 입사자가 기업 이메일에 액세스하기 전에 먼저 가상 계정 관리 세션을 호스팅하여 설정 지침을 입사자의 개인 이메일 주소로 발송합니다.

8. 단계별 배포 후 검토 및 수정 준비

복잡한 배포와 정책이 처음부터 완벽한 경우는 거의 없습니다. 전 직원에게 영향을 미칠 정도로 프로세스를 변경해야 하는 경우가 있기 때문에 MFA 솔루션을 배포하고 사용하면서 효과를 추적한 후 관찰 결과를 바탕으로 정책을 개선하는 것이 좋습니다. 이상적으로는 IT/보안 팀이 MFA를 처음 사용할 때 단계별로 배포하는 것입니다. 이후부터 사용자 그룹을 추가하여 확장하면 됩니다. 프로세스 초기 단계부터 감사 기능을 사용하는 것에 익숙해지십시오. 이는 정책 구성 문제를 해결하고 조정하는 데 매우 중요한 역할을 할 것입니다. 사용자에 대한 MFA 배포를 마쳤다면 이제 감사 툴을 이용해 사용 현황을 수시로 확인하십시오. 사용자가 피드백을 알릴 수 있는 메커니즘 역시 좋은 생각입니다. 사용자가 간혹 피드백을 작성해서 제공할 만한 시간이 충분하지 않다면 감사 추적을 통해 사용자 경험을 어느 정도 분석할 수 있습니다. 사용자가 3회 시도 끝에 OTP를 입력했습니까? 아니면 포기했습니까? 이러한 문제는 구성 오류, 사용자 교육의 허점 또는 초기 배포 계획 수립 시 생각하지 못했던 시나리오 등에서 비롯될 수 있습니다. 이렇게 감사 툴을 사용하고 직원들에게 피드백을 권장하면 시스템이 정상적으로 작동하고 새로운 보안 정책이 성공적으로 적용되고 있다는 것을 모든 이해관계자가 알 수 있습니다.

보너스: 적응형 MFA 도입

이번 팁은 처음에 시작할 때 효과적입니다. 단계별 MFA는 MFA의 적용 방법과 시기를 상세히 제어할 수 있다는 이점이 있지만 구성할 때 신중하게 생각해야 합니다. 아무리 세심하게 결정한 정책과 기준이라고 해도 사용자 또는 디바이스 컨텍스트의 변화에 따라 즉시 결단을 내려야 할 때도 있습니다. 동적 변경 기능을 활용하고 싶다면 **Okta의 Adaptive MFA** 솔루션을 추천합니다. Adaptive MFA는 액세스 패턴을 인지한 후 각 사용자나 그룹에 대한 정책을 조정합니다. 예를 들어 자주 출장을 가고 해외에서 이메일을 확인하는 직원은 주기적으로 2차 인증 요소가 필요할 수 있습니다. 하지만 출장을 전혀 가지 않는 직원이라면 필요한 경우에만 즉석에서 MFA 입력을 요구하는 것이 좋습니다. 또한 권한이 없는 프록시를 통해 리소스에 대한 액세스를 시도할 때 단계별 인증을 요구하거나, 알려진 악성 IP의 액세스를 자동으로 차단하는 등의 위험 기반 정책 역시 의심스러운 이벤트가 발견되었을 때 작동할 수 있습니다. Adaptive MFA는 시간이 지나면서 정책을 자동으로 조정하여 기업이 원하는 보안 환경을 구현할 만큼 충분히 엄격하며, 각 사용자에게 적용될 만큼 충분히 유연한 정책을 설정할 수 있다는 점에서 매우 강력한 도구입니다.

안전한 다중 요소 인증 구축

엔지니어링 및 제품 책임자를 위한 세 가지 모범 사례

서론

전자 시스템의 보안 인증 설계 방법과 관련하여 다양한 책들이 출판되었습니다. 이에 지금까지 엔지니어링 및 제품 팀과 협력하면서 쌓아온 노하우를 바탕으로 애플리케이션용 MFA 솔루션 개발자에게 실질적으로 도움이 될 만한 정보를 소개하고자 합니다.

다음은 MFA 기능의 보안을 강화하는 세 가지 방법입니다.

1. 계정 복구 프로세스의 취약점 분석 및 관리
2. 무차별 대입 공격에 대한 로그인 프로세스 보호
3. 위험, 사용 편의성, 비용 간 절충 효과를 관리할 수 있는 설계. 여기에서는 비밀번호가 유출되었다고 가정하고 이러한 관점에서 2차 요소를 살펴보겠습니다.

계정 복구 프로세스의 취약점 분석 및 관리

다중 요소 인증의 안전성은 계정 복구 프로세스에 달려 있다고 해도 과언이 아닙니다. 최근에 크게 알려진 사고들을 보면 공격자들은 계정 복구 프로세스의 취약점을 이용해 계정을 제어할 수 있었습니다. Acme 웹 애플리케이션의 경우 사용자의 휴대전화에 설치된 소프트 토큰 앱을 기반으로 MFA를 제공하여 사용자가 소프트 토큰에 액세스할 수 없을 경우 등록한 전화번호를 통해 백업용 2차 인증 요소를 받아 계정 복구에 사용할 수 있도록 지원합니다. 따라서 Acme의 2차 요소는 이동통신 사업자의 고객 인증 프로세스와 통화/SMS 발신 프로세스에 따라 유효성이 결정됩니다. 과연 공격자가 사용자를 사칭하여 수신되는 전화 통화 또는 SMS를 자신이 제어하는 번호로 연결하도록 고객 서비스 담장자를 설득하거나 요구할 수 있을까요? 모든 2차 요소는 대체 방법이 필요하기 때문에 '안전한 복구 프로세스를 개발하려면 어떻게 해야 하는가'라는 질문을 떠올리게 됩니다. 여기 안전한 2차 요소 복구 프로세스를 설계하기 위한 팁을 소개합니다. 다만 상황에 따라 접근 방식이 다양하다는 점을 염두에 두시기 바랍니다.

1차 요소와 2차 요소의 독립성

2차 요소 복구와 1차 요소 복구를 분리합니다. 공격자가 1차 인증 요소에 액세스하여 비밀번호를 이용해 리셋할 수 있게 된다면 2차 요소는 무용지물이 됩니다. 나아가 2차 요소 복구 프로세스는 비밀번호 복구 프로세스와 완전히 분리되어야 합니다. 예를 들어 이메일 메시지가 비밀번호를 복구하는 방법이라면 2차 요소를 복구할 때는 완전히 분리된 채널을 이용해야 합니다.

관리자 개입

관리자는 여러 가지 시나리오에서 안전을 보장할 수 있는 인증 방법을 정교하게 구현할 수 있습니다. 기업 시나리오에서 기업은 직원의 업무나 프로필 내용을 비롯해 회사 및 인간 관계에서 가져온 공유 비밀 정보를 통해 직원을 인증하는 데 유리합니다.

한 가지 눈여겨 볼 접근 방식은 직원의 관리자에게 사용자 인증을 요청한 후 IT 팀에게 MFA 리셋 권한을 부여하는 것입니다. 소비자 시나리오에서는 관리자가 대량의 공유 비밀 정보에서 사용자 정보를 얻을 수 있습니다. 예를 들어 신규 소비자로 등록되면 소비자 금융 애플리케이션이 잘 알려지지 않은 대규모 개인 정보를 수집하고, 이렇게 수집된 정보는 향후 계정 복구를 위한 공유 비밀 정보로 사용됩니다. 애플리케이션이나 회사와 관련된 개인 이벤트 역시 공유 비밀 정보로 사용될 수 있습니다. 또한 공유 비밀 정보는 웹이나 음성을 통한 자동 평가가 가능하기 때문에 대부분의 경우 사회 공학에 대한 취약점을 완화하여 사람이 구성하는 것보다 더욱 안전한 보안 환경을 보장할 수 있습니다.

백업용 2차 요소 제공

대부분의 시나리오는 2차 요소를 자동으로 복구하는 방법이 필요합니다(다수의 사용자에게 제공되는 제품이지만 1:1 지원 비용이 만만치 않은 경우, 운영 비용을 줄여야 하는 경우 등). 신규 사용자 등록 시 2차 요소를 2개 이상 적용하면 사용자가 백업용 2차 요소를 통해 인증을 완료하여 2차 요소를 복구할 수 있습니다. 저렴한 비용으로 간편하게 적용할 수 있는 방법이 있는데, 바로 사용자에게 백업용 2차 요소로 사용할 수 있는 일회성 코드가 다수 저장된 (실물 또는 인쇄 가능한) 카드를 제공하는 것입니다.

무차별 대입 공격에 대한 로그인 프로세스 보호

저렴한 컴퓨팅 리소스가 널리 사용되면서 무차별 대입 공격에 대한 인증 시스템의 취약점도 증가하고 있습니다. 하지만 몇 가지 간단한 기법을 사용하면 비밀번호가 유출된 상황에서도 MFA 보안을 크게 강화할 수 있습니다.

로그인 프로세스 시퀀스, 최대 시도 횟수, 계정 잠금

2차 요소를 요구하는 페이지를 로그인 페이지에 연이어 설계하면 다음과 같은 두 가지 이점이 있습니다. 최대 로그인 시도 횟수에 도달하여 로그인에 실패하게 되면 계정 잠금 공격으로부터 사용자를 보호합니다(최대 로그인 시도 횟수가 1차 요소에 적용되었을 때). 둘째, 잘 알려지지 않은 2차 요소를 사용하면 공격자가 다른 보안 계층에 대한 가시성을 잃게 됩니다. 2차 요소에 시도 횟수 제한 및 잠금 정책을 구현합니다. 사용자가 토큰을 여러 차례 잘못 입력할 가능성은 낮기 때문에 실패 횟수가 늘어날수록 공격에 대한 의심은 확신으로 바뀝니다. 단위 시간마다 가능한 전체 시도 횟수를 줄이려면 액세스를 시도할 때마다 응답 시간을 늘려야 하는데, 액세스 시도가 여러 차례 실패할 경우 계정을 완전히 잠그는 기능(가능한 경우)도 필요합니다. 시간 기반 2차 요소의 경우에는 토큰 수명에 따라 최대 시도 횟수를 관리합니다.

로그 및 알림

실패한 2차 요소 시도를 수집하여 분석합니다. 2차 요소를 입력하는 시도에서 여러 차례 실패할 경우 사용자 또는 관리자에게 의심스러운 동작을 알리고 사용자에게 새로운 토큰을 등록하도록 요청합니다.

- 대역 외 토큰 사용

  1차 요소와 분리된 채널을 통해 확인된 2차 요소는 무차별 대입 공격(및 피싱)에 대한 보안을 더욱 강화하는 효과가 있습니다. 예를 들어 많은 사람들이 사용하는 요소를 새롭게 적용하여 인증 요청에 대한 세부 정보와 요청을 허용하거나 거부하는 프롬프트 메시지를 휴대전화 푸시 알림과 함께 사용자에게 전송합니다. 기존 무차별 대입 공격으로는 이러한 채널에 접근하지 못합니다.

위험, 사용 편의성 및 비용을 관리할 수 있는 설계

다중 요소 인증 기능의 설계는 어떤 맥락에서든지 보안, 사용 편의성, 그리고 비용에 엄청난 영향을 미칩니다. 보안에 치중한 2차 요소는 경우에 따라 번거로운 일이 늘어나 엔드 유저와 관리자에게 부담을 가중시키기 때문에 MFA를 제품에 도입하는 데 영향을 미쳐 결국 보안 수준 저하를 초래할 수 있습니다. 여기 위험, 사용 편의성 및 비용을 적절하게 조합할 수 있는 몇 가지 모범 사례를 소개합니다.

- 다원화된 사용자에게 서비스를 제공할 수 있는 광범위한 옵션 제공

  사용자 계층이 다양해지면서 위험 수준 또한 다양해졌고, 이에 따라 안전을 보장할 수 있는 수준도 달라졌습니다. 관리자의 경우 개인 사용자보다 액세스 범위가 훨씬 넓기 때문에 더욱 강력한 2차 요소를 제공하는 반면, 사용자에게는 더욱 편리한 옵션을 제공하는 것이 좋습니다. 소비자 시나리오에서는 사용자에 따라 자신의 계정에 적용하려고 하는 보안 설정도 다릅니다. 경우에 따라 안전 보장 범위를 낮추고 편의성을 높인(실제로 사용되는) 옵션(SMS 등)이 안전 보장 범위를 높여 오히려 도입을 저해하는 옵션보다 더욱 강력한 보안을 제공하기도 합니다.

- 페더레이션 인증 지원

  기업 시나리오의 경우, 다수의 기업들이 관리하는 아이덴티티에 따라 로컬에서 인증 및 MFA 솔루션을 구현하여 각 리소스에게 페더레이션하고 있습니다. 이러한 접근 방식에서는 제품 개발 팀이 정책 및 보안 프로세스 관리를 고객에게 위임할 수 있습니다. 고객이 MFA를 개별적으로 구현하게 되면서 앞서 언급했던 사항을 고려하여 자신의 특정 환경이나 제약에 맞게 최적화할 수 있습니다. 예를 들어 고객은 자신의 특정 IT 역할에 따라 계정 복구 관리를 설계할 수 있습니다. 이러한 위임 방식에는 사용자가 토큰 하나로 모든 리소스에 액세스할 수 있다는 이점이 있습니다.

결론

MFA 성공을 향한 로드맵

요약하자면, 다중 요소 인증은 애플리케이션 개발자가 자신의 애플리케이션에 대한 액세스 보안을 강화할 수 있다는 점에서 매력적인 방법입니다. 다만, MFA 보안을 위해서는 2차 요소 복구 프로세스를 분석하고 무차별 대입 공격을 차단할 수 있도록 설계하며, 보안, 사용 편의성 및 비용을 적절하게 조합하는 등 여러 단계를 거쳐야 합니다.

오늘날 MFA에 대한 자동화 접근 방식은 자격증명에 대한 제어를 통해 데이터 유출 위험을 크게 줄이는 데 효과적입니다. 그렇다면 기업은 무엇부터 시작해야 할까요?

다음과 같은 주요 단계를 중심으로 시작하는 것이 좋습니다.

1. 가능한 경우 비밀번호 제거
2. 그 밖의 경우 강력하고 독자적인 비밀번호 사용
3. 1차 요소와 2차 요소 분리를 통한 계정 복구 프로세스 보호
4. 단계별 인증으로 주요 애플리케이션의 보안 강화
5. 온프레미스, 클라우드 및 모바일 애플리케이션에 통합 정책 적용
6. 정확한 권한 할당을 통한 프로비저닝 자동화
7. 대규모 디프로비저닝과 가시성 및 보고 활성화
8. 인증 이벤트가 발생할 때마다 중앙에서 실시간 보고 및 알림 메시지 배포
9. 아이덴티티 관리 전략과 기존 보안 툴의 통합
10. 파트너, 공급업체 및 계약자를 추가하여 아이덴티티 및 다중 요소 인증 확대

MFA에 Okta를 사용해야 하는 이유

아이덴티티 관리에 대한 Okta의 최신 접근 방식은 기업이 아이덴티티와 다중 요소 인증을 모두 제어하여 데이터 유출을 줄일 수 있다는 점에서 독보적입니다. Okta의 다중 요소 인증에서 얻을 수 있는 이점

기업 인력과 고객에 대한 빠른 MFA 활성화

- Okta 애플리케이션 네트워크에서 즉시 이용할 수 있는 5,000개의 연결점을 통해 MFA를 쉽고 빠르게 배포합니다.
- RADIUS, RDP, ADFS, LDAP는 물론이고 Okta Access Gateway를 통해 헤더 기반 인증과 Kerberos까지 지원하여 온프레미스 애플리케이션으로 적용 범위를 확장합니다.
- 디바이스 및 연결 속성를 기반으로 컨텍스트에 따라 액세스를 지능적으로 손쉽게 결정합니다.

하지만 데이터 유출을 포괄적으로 차단하려면 강력한 인증만으로 부족합니다. Okta는 다음과 같은 기능을 손쉽게 지원합니다.

아이덴티티의 중앙화

- 계정 관리의 복잡성을 완화합니다.
- 사용자가 비밀번호를 줄일 수 있도록 액세스를 통합하는 동시에 간소화합니다.
- 지능적인 SAML 연결을 통해 서비스에 대한 액세스를 제한하여 위험을 완화하고 아이덴티티의 무분별한 확산을 줄입니다.

공격 대상 감소

- 프로비저닝 및 디프로비저닝의 자동화로 일관된 입사자 계정 관리를 촉진하는 동시에 사용자가 없는 계정을 방지합니다.
- SCIM과 SDK, 그리고 Okta의 API를 통해 맞춤형 애플리케이션을 확장합니다.
- 완전한 라이프사이클 관리로 액세스 요청 워크플로에 따라 해당하는 권한을 부여하여 필요한 애플리케이션에 액세스할 수 있습니다.

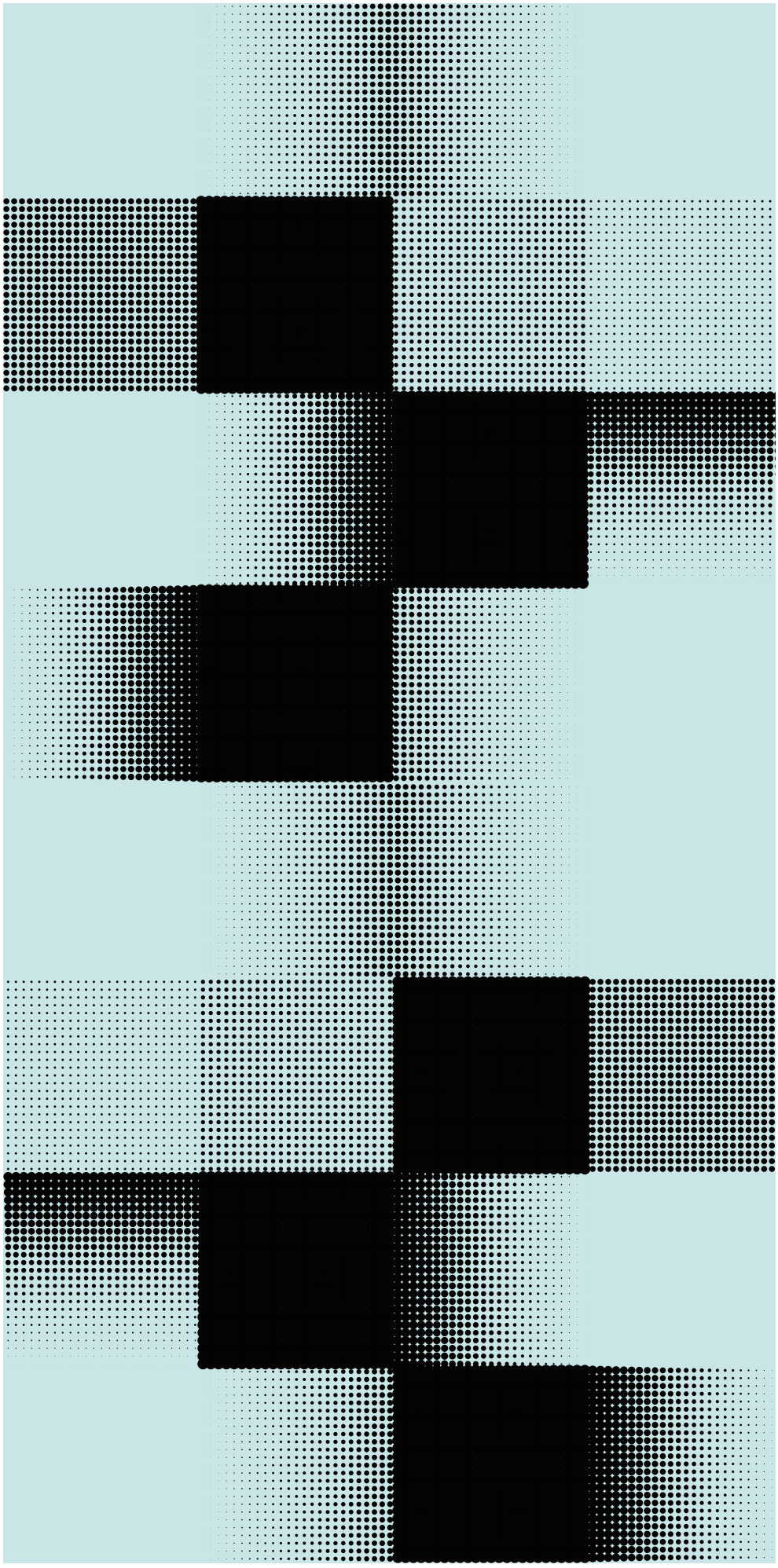
계정 침해 시 신속하게 대응

- 프로비저닝 및 디프로비저닝의 자동화로 일관된 입사자 계정 관리를 촉진하는 동시에 사용자가 없는 계정을 방지합니다.
- SCIM과 SDK, 그리고 Okta의 API를 통해 맞춤형 애플리케이션을 확장합니다.
- 완전한 라이프사이클 관리로 액세스 요청 워크플로에 따라 해당하는 권한을 부여하여 필요한 애플리케이션에 액세스할 수 있습니다.

Okta의 Adaptive MFA 솔루션을 손쉽게 관리하는 방법과 인증 프로세스 시범 운영을 원하신다면 **이 데모를 시청하십시오**.

Okta 소개

Okta는 기업 아이덴티티 분야의 독자적인 선두 기업입니다. Okta Identity Cloud는 기업들이 사람과 테크놀로지를 적시에 안전하게 연결할 수 있도록 지원합니다. 6,500개 이상의 애플리케이션 및 인프라 공급업체가 사전에 통합되어 있어 Okta 고객들은 자신의 비즈니스에 가장 적합한 테크놀로지를 손쉽고 안전하게 사용할 수 있습니다. 또한 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America, Twilio 등 8,950개 이상의 기업들이 Okta를 통해 자사 인력 및 고객의 아이덴티티를 보호하고 있습니다. 자세한 내용은 **okta.com**을 참조하십시오.



okta