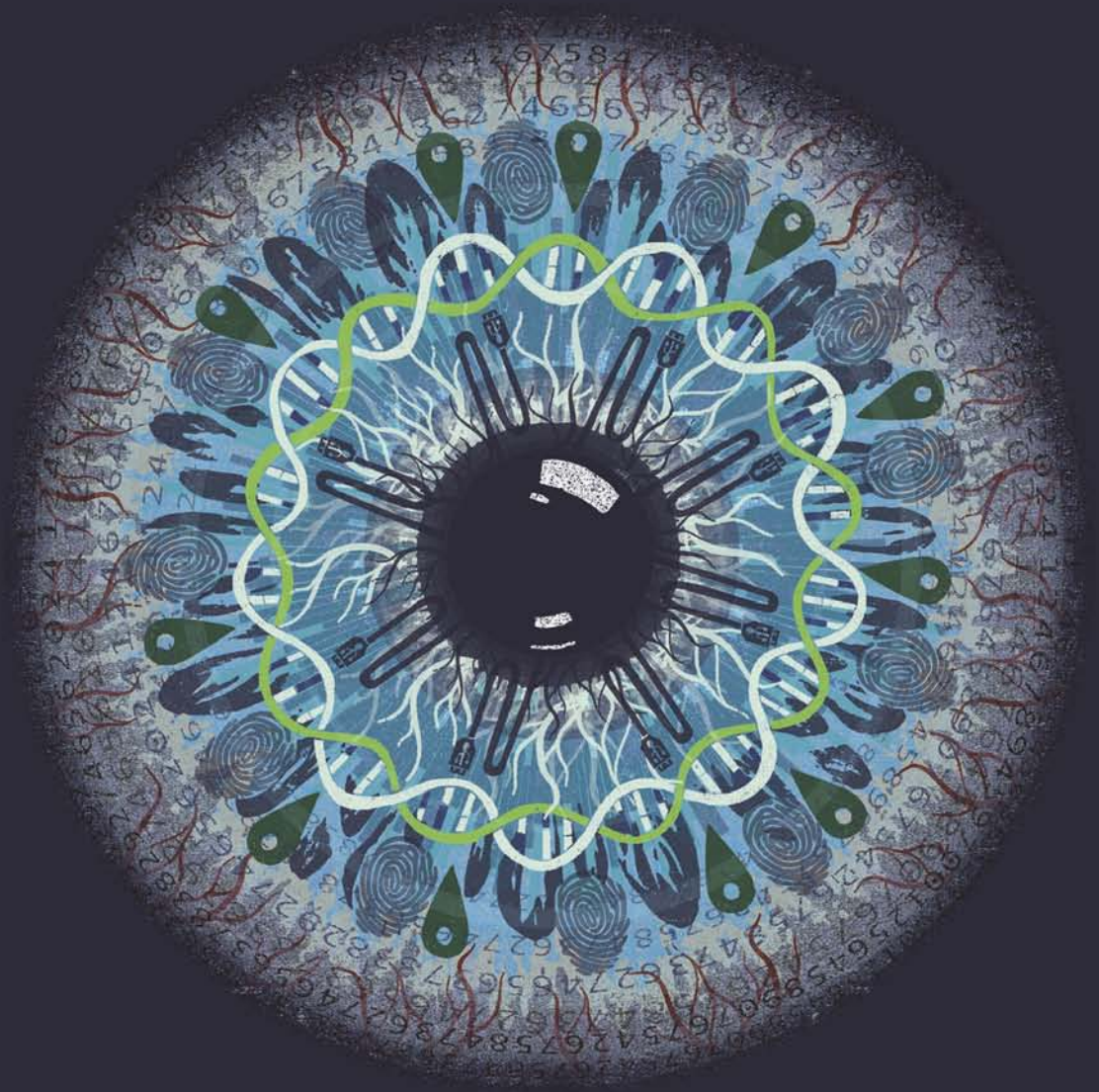


비밀번호 너머의 세상

디지털 변환의 시대에서 보안, 효율성, 사용자 경험을 개선하기

저자 Mike Wyatt, Irfan Saif, David Mapgaonkar
일러스트레이션 Lucy Rose

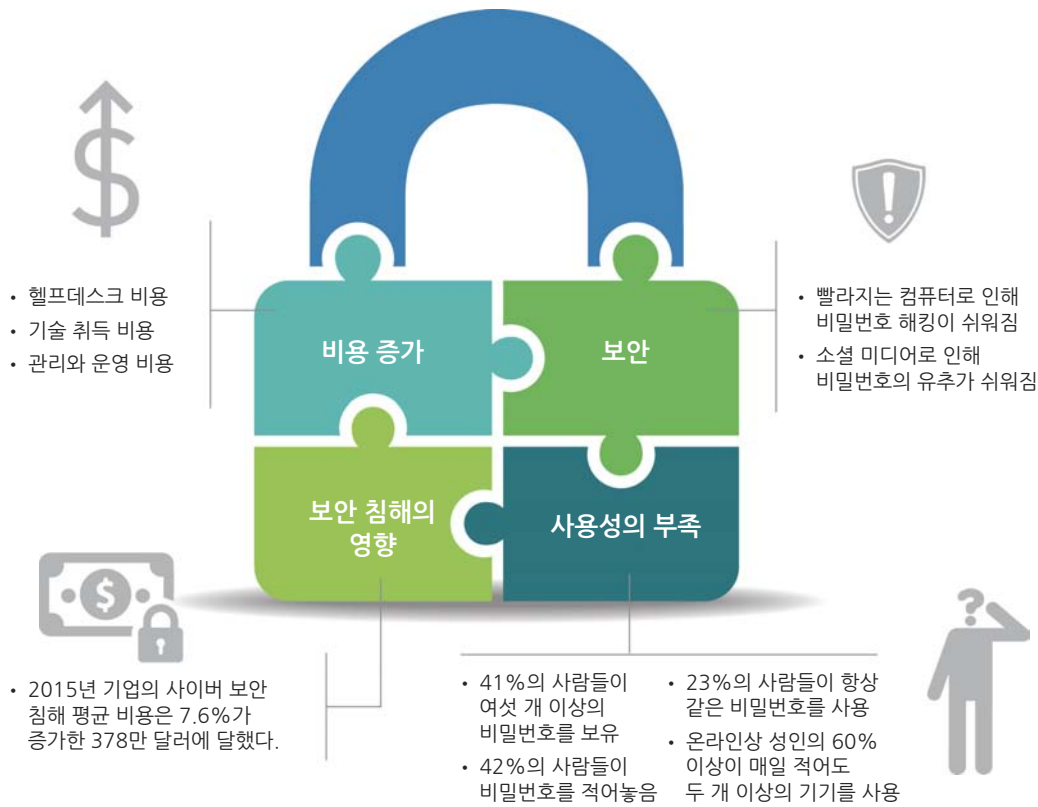
당신이 컴퓨터를 통해 민감한 재무 정보(합병 등)에 접근하려 할 때, 몇 주전에 이 특정 사이트를 위해 만들었던 비밀번호, 즉 알파벳 대문자, 소문자, 숫자, 특수문자 등으로 조합된 비밀번호를 기억할 필요가 없다고 가정해보자. 사용자명과 비밀번호의 입력을 요구하는 대신에 웹사이트는 당신이 어제 점심을 먹었는지 질문하고, 동시에 당신의 스마트워치가 사용자의 고유한 심박 신호를 검증한다. 이 과정은 더 나은 사용자 경험을 제공할 뿐 아니라 더 안전하다. 당신의 고유 정보를 사용한 접근법은 당신이라고 주장하는 사람이 정말 당신인지 확인하는 데 있어 비밀번호 시스템보다 더 뛰어나고 강건하다.

급변하는 디지털 기술은 오늘날 대부분의 기업 전략의 초석이며, 디자인 철학의 중심이 된 사용자 경험(UX)이 이 변환의 동력이다. 하지만 고객, 비즈니스 파트너, 일선의 직원, 임원에게 있어 대부분의 사용자 경험은 번거롭고 보안적 측면에 있어 가장 약한 고리인 트랜잭션(Transaction) 과정과 함께 시작한다. 실제로 기업이 받은 사이버 공격 중 3/4 이상의 취약하거나 도용 당한 비밀번호가 원

인이었다.[1] 모든 독자가 알고 있듯 기업의 사이버보안 침해는 기술, 법률, 홍보 등에서 수백만 달러의 비용을 초래한다. 그리고 덜 구체적이지만 더 타격이 큰 피해로서 평판 혹은 신용 등급의 하락, 계약 취소, 기타 비용 등이 발생할 수 있다.[2] 비밀번호의 취약성이 개선되면 기업의 사이버 리스크가 상당히 줄어들 것이다. 뿐만 아니라 사용자의 생산성이 증가하고, 고객의 호감도가 증가하며, 직원들의 비밀번호 분실과 계정 접근 차단을 주기적으로 관리하기 위해 소요되는 시스템 관리 비용도 줄어들 것이다.

CIO 뿐만 아니라 점점 길어지는 비밀번호를 외우는 데 지친 사람들에게 좋은 소식이 있다. 생체인식과 사용자 애널리틱스, 사물인터넷 적용 등 새로운 기술이 기업에 양자간 신뢰, 사용자 경험, 개선된 시스템 보안을 기반으로

그림 1.비밀번호의 문제점



출처: 로보폼(RoboForm), "비밀번호 보안 설문조사 결과 - 파트 1(Password security survey results-part1)"," http://www.roboform.com/blog/password-security-survey-results, 2016.04.21 ; 필립 잉겔산트(Philip Inglesant) M.안젤라 사쎄(M. Angela Sasse), "사용할 수 없는 비밀번호 정책의 진짜 비용: 실제 환경에서 비밀번호 사용(The true cost of unusable password policies: Password use in the wild)" 컴퓨팅 시스템에서의 인간 요소에 대한 SIGCHI 컨퍼런스의 의사 진행(2010): pp. 383-392; 포탈가드(PortalGuard), 복수의 비밀번호 요구와 연관된 실제 비용 Top 10(Top 10 real costs associated with requiring multiple passwords), 2011; 탐 리조(Tom Rizzo), "비밀번호의 진짜 비용(The hidden costs of passwords)", 스콜피온소프트(ScorpionSoft), 2015.8.20, http://insights.scorpionsoft.com/the-hidden-costs-of-passwords; 빅토리아 울라스톤(Victoria Woollaston), "강력한 비밀번호를 가지고 있다고 생각하는가? 해커는 16자리 비밀번호를 1시간 내에 풀 수 있다(Think you have a strong password? Hackers crack 16-character passwords in less than an HOUR)", 데일리 메일(Daily Mail), 2013.05.28; 맷 스미스(Matt Smith), "패스워드 해킹을 위해 사용되는 가장 보편적인 5가지 방법(The 5 most common tactics used to hack passwords)", 2011.12.20, http://www.makeuseof.com/tag/5-common-tactics-hack-passwords/; 포네몬 인스티튜트(Ponemon Institute), 2015 데이터 침해 비용 연구: 글로벌 분석결과(2015 cost of data breach study: Global analysis), 2015년 5월; 올리 로빈슨(Olly Robinson), "다수의 기기로 가득한 세상에서 단순성 찾기(Finding simplicity in a multidevice world)", Gfk 인사이트 블로그, 2014.05.06, http://blog.gfk.com/2014/03/finding-simplicity-in-a-multi-device-world/.

그래픽: Deloitte University Press | DUPress.com

새로운 패러다임을 설계할 수 있는 기회를 제공하고 있다. 이의 성공적인 실행은 사업의 빠른 성장과 시장에서 기업의 차별화에 도움을 줄 수 있다.

사실, 계정과 비밀번호 없이 안전하게 디지털 정보에 접근하는 방식의 업그레이드는 일과 삶의 측면에서 오랫동안 지연되어 왔다. 비밀번호는 사용자들이 기대하는 완전한 디지털 경험을 제공하기에는 확장성이 부족하다. 특히 오늘날 사용되는 수많은 온라인 애플리케이션들을 지원하는 데 필요한 확장성이 부족하다. 그리고 사용자가 더욱 기대하고 요구하는 매끄러운 사용자 경험(UX)을 제공하지도 않는다. 그 결과 사용자들은 불가피하게 권고를 무시한 채[3] 동일한 비밀번호를 계속 사용한다. 이로 인해 접속하는 모든 시스템들의 취약성이 증가한다. 아마 더 중요한 점은 비밀번호가 거래 가치에 상응해 맞춤화된 인증 대응을 제공하는 확장성이 부족하다는 사실일 것이다. 즉, 문자 사용이나 비밀번호 길이에 대해 번거로운 정책을 요구하는 강력한 비밀번호 시스템은 시스템 관리자들이 주어진 비밀번호의 강도를 평가할 수 없게 만든다. 이러한 지식이 없으면, 기업은 어떻게 다른 인증 요소들로 비밀번호를 계층화해야 할 지 리스크 정보에 기반해 결정하기가 어려워진다.

21세기가 인간의 한계에 부딪히다

20년 전의 전형적인 소비자라면 이메일용으로 단 하나의 비밀번호만을 가지고 있었을 것이고, 이는 아마도 은행계좌 비밀번호와 똑같은 4자리 숫자였을 것이다. 오늘날 온라인 사용자는 며칠마다 새로운 계정을 생성한다. 그리고 각 사이트는 기업 정보 접근부터 온라인 쇼핑, 가스/전기요금 납부, 투자 확인, 10km 단축마라톤 참가 등록, 단순히 회사 이메일에 로그인하는 데까지 복잡한 비밀번호를 요구하는 듯 하다. 일각에서는 2020년까지 사용자마다 200여개의 온라인 계정을 가지게 되고, 각 사이트마다 고유한 비밀번호를 요구할 것이라고 예측한다.[4] 최근 설문조사에 따르면 응답자의 46%가 이미 10개 이상의 비밀번호를 가지고 있다고 답했다.[5]

그림 1이 보여주듯 비밀번호의 보안 요구는 인간 능력의 한계를 향해 가고 있다. 심리학자 조지 밀러(George Miller)에 따르면 인간이 가장 잘 기억하는 숫자는 일곱 자리이며, 여기서 두 자리 정도가 많거나 적다고 한다.[6] 수준급 해커가 여덟 자리 비밀번호를 77일만에 풀 수 있는 이 시대에는 아홉 자리 비밀번호를 90일마다 바꾸는 정책이어야 충분히 안전하다 할 수 있을 것이다.[7]

하지만 이렇게 긴 비밀번호는 특히 정기적으로 여러 개를 바꿔야 할 때, 사람들의 기억력에 부담을 주게 된다. 이에 따른 불가피한 결과는 다음과 같다. 사람들은 취약한 같은 비밀번호를 여러 계정에 다시 사용하고, 비밀번호가 적힌 메모를 컴퓨터 모니터에 붙여놓으며, 비밀번호를 공유하고, 자주 홈페이지의 비밀번호 찾기 기능에 의존한다. 최근 미국과 영국의 사용자들을 대상으로 실시한 설문조사에서 23%가 언제나 동일한 비밀번호를 사용한다고 답했고, 42%는 비밀번호를 적어놓는다고 말했다. 응답자의 74%가 하루에 6개 이상의 웹사이트나 애플리케이션에 로그인하는 반면, 단지 41%만이 6개 이상의 고유한 비밀번호를 사용했다.[8] 또 다른 설문조사에 따르면 사용자의 20% 이상이 일상적으로 비밀번호를 공유하고, 56%는 개인 계정과 회사 계정에 동일한 비밀번호를 사용했다.[9] 비밀번호 관리 소프트웨어가 이 문제를 일부 경감해주기는 하지만, 여전히 궁극적으로는 비밀번호의 조합이 중요하다.[10]

직원이 모든 규정을 준수하고 독특하며 보안수준이 높은 서로 다른 비밀번호 6개를 기억한다고 해도 여전히 비밀번호는 취약하다. 인간은 여전히 비밀번호를 탈취 당하거나 누설하도록 꾐에 빠질 수 있다. 악성소프트웨어인 멀

웨어(Malware)가 컴퓨터에 설치되어 있거나, 사이버 범죄자가 로그인 정보나 신용카드, 기타 데이터를 합법적인 것처럼 보이는 웹사이트나 앱을 통해 훔쳐가는 피싱(Phishing)도 있다. 소프트웨어의 취약성을 해커가 악용하는 "제로데이(Zero Day)" 공격도 존재한다.[11] 물론 고전적인 방식의 인간적 공격도 계속된다. 사용자가 비밀번호를 입력할 때 어깨 너머로 슬쩍 본다든지, 버려진 비밀번호 정보를 찾기 위해 쓰레기통을 뒤지거나, 부하 직원들로부터 비밀번호를 입수하기 위해 회사의 고위직인 듯 행세하기도 한다. 소셜 미디어 계정의 비밀번호를 바꾸기 위해 개인에 대한 정보를 파악해내는가 하면, 직원들이 회사의 비밀번호를 매매하기도 한다.

물론 비밀번호를 유지하기 위한 운영 비용도 발생한다. 비밀번호를 잊어버린 사람들을 위한 헬프데스크, 잘못된 비밀번호를 여러 번 입력해 발생하는 계정 잠금으로 인한 생산성 하락, 그 외에도 여러 가지 문제로 인한 비용이 증가하고 있다. 더욱 걱정스러운 점은 점점 강력해지는 컴퓨터의 능력이 무작위로 문자를 마구 대입해 암호를 추측하는 새로운 무차별 대입 공격(Brute-force attack)을 가능하게 한다는 사실이다. 비밀번호의 미래는 비용이 많이 들고 불안하다.

- 설문대상 응답자의 74%가 하루에 여섯 개 이상의 웹사이트와 애플리케이션에 접속한다고 답했다.[12]
- 설문대상 직원의 20%가 일상적으로 비밀번호를 공유한다고 답했다.[13]
- 설문대상 직원의 56%가 개인 계정과 회사 계정에 동일한 비밀번호를 사용한다고 답했다.[14]

위치인식에서 생체인증까지

기업의 리더는 정보와 접근 전략이 오늘날 거의 모든 비즈니스의 핵심이라는 점을 잘 인지하고 있다. 이제는 이 전략을 시행하기 위해 역사적으로 사용돼왔던 기제, 즉 비밀번호가 근본적으로 망가졌다는 점을 인식해야 한다. 그들의 신탁책임과 지배책임을 고려할 때 이사회와 최고경영진은 보다 강건한 온라인 접속 보안을 제공해 기업의 보물 창고—디지털 정보—를 보호해야 할 책임을 주주들에게 지고 있다. 결국 투자자, 고객, 직원, 협력업체, 제삼자 판매인, 기타 관계자들은 강력한 기업정보보호를 통해 정당한 사용자에게 정보에 더 쉽게 접근할 수 있는 혜택을 누릴 것이다. 이같이 양자간 신뢰를 강화하는 것이 모든 건전한 비즈니스 관계의 핵심이다.

소비자, 직원, 협력사 모두가 매끄러운 디지털 상호작용을 점점 더 기대함으로 인해, 기업이 사용자 신원에 대해 구상하고, 사용하며, 관리하는 방법에 대한 근본적인 패러다임의 변화가 일어나고 있다. 이러한 변화에 따라 새로운 로그인 자격 증명은 단지 "당신이 무엇을 아는가" 혹은 특정 비밀번호뿐만 아니라 "당신은 누구인가," "당신은 무엇을 가졌는가," "당신은 어디에 있는가," 그리고 "당신은 무엇을 하고 있는가"까지 포함해 구성될 수 있다. 여기에는 개인이 특정 정보에 접근하는 시점과 요일에 대한 개인의 패턴 탐지, 사용자 행동 특성의 기타 동적인 맥락 평가, 개인의 위치, 생채인증, 토큰 등이 포함될 수 있다. 인증에 의존하는 시스템은 적응성을 갖춰가고 있으며, 만약 사용자의 일반적인 사용 패턴과 다를 경우에는 심지어 기본적인 인증자격이 맞는 듯한 경우라도 그 인증 시도가 너무 위험하다고 표시할 수 있다. 그런 경우 시스템은 인증을 강화해 사용자에게 신원 증명을 위한 추가적인 증거를 요구할 수 있다. 오늘날 누구나 휴대전화를 가지고 있기 때문에 휴대전화는 인증에 사용할 수 있는 가장 확실한 기기다. 하지만 벤처 투자자들은 또한 다른 연결 기기의 개

고대 그리스에서 디지털 시대까지

고대부터 비밀번호는 지금과 같은 목적으로 사용됐다. 즉 보호받는 자산에 접근할 수 있는 사람들의 자격을 부여하기 위한 수단이었다. 이런 식의 권한 설정은 등록된 값과 대조하는 "인증"을 위해 "당신이 아는 무엇(What you know)", 즉 비밀번호를 제시하는 방식에 달려있다. 그림 2가 보여주듯이 비밀번호는 지난 50년 간의 디지털 열쇠로서의 역할을 포함해 우리 역사의 초석이었다. 실제로 디지털 비밀번호는 장점이 있었다. 간단하고 사용하기 쉽고 비교적 편리했던 것이다. 만약 유출되면 변경도 가능했고 비록 보안을 손상시키는 행위긴 하지만 편리하게 비밀번호를 공유할 수 있었다. 비밀번호가 지배적인 표준이기 때문에 이를 관리하는 기업 정책이 잘 수립되어있다. 그리고 신원 확인과 접속 관리 시스템도 이를 지원한다.

그림 2. 비밀번호의 역사

출처: 브라이언 블랙(Bryan Black), "스파이 활동의 언어: 신호, 역신호, 그리고 인식(The language of espionage: Signs, countersigns, and recognition)", 이미넌트 쓰레트 솔루션(Imminent Threat Solutions), 2015.08.11; 데이비드 월든(David Walden), 탐 반 블렉(Tom Van Vleck), eds, 호환가능한 시간 공유 시스템(1961-1973): 50주년 기념 개요(The Compatible Time Sharing System (1961-1973): Fiftieth anniversary commemorative overview), IEEE Computer Society, 2011; "비밀번호 보안: 과거, 현재, 미래(Password security: Past, present, future)", 오픈월(Openwall), 2012

그래픽: Deloitte University Press | DUPress.com

발에 투자하고 있다. 예를 들어 개인의 고유한 심장박동을 확인하는 손목 밴드, 인간이 비밀번호를 입력할 필요 없이 기계간 인증을 수행하는 USB 동글(역주: 컴퓨터의 I/O 포트에 연결되는 장치로 특정 프로그램의 복사나 실행 시 인가된 사용자만이 사용할 수 있도록 보안 키나 ID를 저장한 장치) 등이 있다.[15]

여러 기술들이 전체적인 시스템 정비를 위해 융합되고 있다 "기술적인 측면에서, 우리는 비밀번호 외에도 여러 가지 놀랍고 새로운 인증 방식들과 분석을 통해 정보에 기반한 결정을 수행할 수 있는 컴퓨터 역량을 보유하고 있습니다." 아이덴티티 이코시스템 스티어링 그룹(Identity Ecosystem Steering Group)의 경영 협의회 부의장인 이안 글레이저(Ian Glazer)는 말한다. 이는 민간부문이 주도하는 위원회로 미국 연방정부와 공조해 보다 안전한 디지털 인증 체계의 개발을 촉진하고 있다. "가장 큰 난제 중 하나가 또한 해결됐습니다. 즉 스마트폰이라는 형태로 모든 사람들의 손에 인증 플랫폼을 쥐어준 것이죠."[16]

회사 입장에서 기존 시스템에서 새로운 시스템으로의 이전은 결코 쉽지 않다. 하지만 리스크 기반의 분석에 따라 최우선적인 비즈니스 운영에 투자와 실행의 초점을 맞춰 이전을 실행하는 사려 깊은 로드맵을 만들 수 있다. 선별된 대안들의 테스트를 위한 시범 프로그램을 시작하면 회사는 가장 필요한 곳에 성공적인 솔루션을 확장할 수 있다. 대부분의 경우 변화를 위한 로드맵을 시작하는 것이 매우 중요하다. 결국 비즈니스는 지속적인 혁신과 성장이 그 어느 때보다 정보의 정합성에 의존하는 시대에서 운영되고 있기 때문이다.

새로운 문지기들

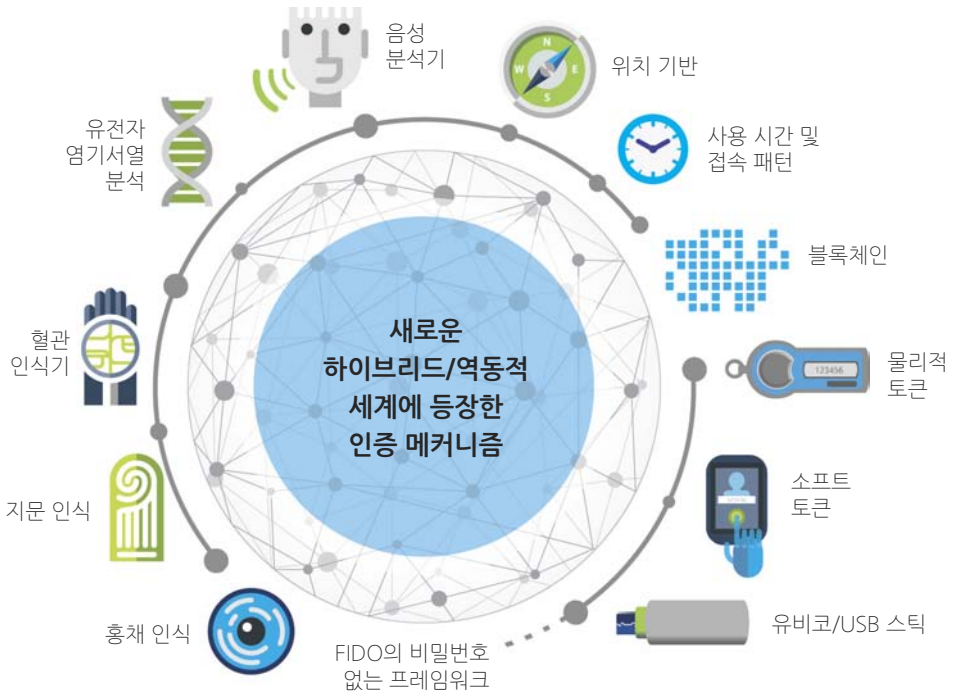
비밀번호 보호에 드는 비용-시간, 리스크, 돈-이 증가하면서 기업은 유연한 리스크 기반의 접근법을 기대하고 있다. 즉 요청되는 트랜잭션의 가치에 상응하는 강도로 사용자 인증을 요구하는 것이다. 다행히 그림 3에서 볼 수 있듯이 기업의 리스크 한도와 사용자 유연성을 동시에 만족시킬 수 있는 방식으로 결합이 가능한 다양한 기술들이 등장하고 있다. 블록체인[17] 같은 신흥 기술이 다양한 요인을 가지고 단일 비밀번호의 취약성을 대체하려 하고 있다.

단계적으로 연결된 다수의 문지기들은 추가적인 점검 단계를 요구해 보안을 강화할 수 있다. 분리된 경로를 통해 서로 다른 신원 증명을 더 많이 요구할수록 절도범은 당신의 신원정보를 훔치거나 당신인 척 가장하기 어려워진다. 마찬가지로 소비자 플랫폼이 디지털 정보에 어떻게 접근할 것인지를 소비자가 선택할 수 있도록 권한을 부여하면서 개선된 사용자 경험을 제공하는 환경을 조성하고 있다.

문자, 공유, 모바일 앱 경제는 즉각적이고 매끄러운 온라인 커뮤니케이션과 거래를 어디서나 가능하게 했다. 초창기와 반대로 이제는 소비자가 얼리 어댑터이고 기업은 후발주자다. 그래서, 항상 몸에 지니고 다니는 스마트폰이 소비자의 디지털 허브가 되어가면서, 중심 기능을 수행하기에 적절한 위치에 있다. 이미 16-24세 연령층의 대부분이 보안을 온라인 구매 전의 귀찮은 절차로 보고 있고, 생체인식이 비밀번호보다 훨씬 빠르고 편할 것이라고 생각한다.[18] 이러한 추세에 부합해 기술 선도 기업들은 2012년 Fast IDentity Online(FIDO)협의회를 결성했다. 이 협의회의 목적은 개방되고 상호 호환되며 확장 가능한 비밀번호 없는 온라인 인증 시스템에 대한 새로운 기술 표준을 수립하는 것이다.[19]

보안을 유지하고 더 큰 사용자 편의를 제공하기 위해 새롭게 진화하는 로그인 시스템의 핵심 개념은 다중요소인증(Multi-factor authentication)이다. 지메일과 트위터는 이 솔루션을 간단한 형태로 적용하고 있다. 이 회사들은 사용자의 노트북 스크린에 입력하는 기존의 비밀번호와 함께, 사용자의 휴대전화로 발송한 1회용 암호를 추가로

그림 3. 많은 문지기가 존재하는 새로운 세계



그래픽: Deloitte University Press | DUPress.com

입력하게 한다. 사용자가 소유한 두 기기에 걸친 인증으로 보안이 강화된다. 컴퓨터 해커가 보호된 계정에 접속하기 위해서는 사용자의 온라인 비밀번호뿐 아니라 전화에도 접근을 해야만 한다.

서로 다른 기기로 암호를 전송하는 것 외 아직 남아 있는 보호 방범은, 다른 형태의 인증 요소를 사용하는 것이다. 예를 들어 이중인증 절차에서 사용자는 노트북이나 스마트폰에 장착된 카메라로 자신의 홍채를 스캔하는 생체인증을 온라인 은행계좌에 접속하기 위한 첫 번째 단계로 사용한다. 두 번째 단계로 은행은 사용자의 휴대전화로 문자 메시지 질문을 보내서 인증 절차의 마무리를 위한 사용자의 문자 응답을 요구한다.

인증 요소로 가장 인기 있는 새로운 방식들 중 하나는 생체인식 기술로, 어떤 자원에 대한 접근을 위해 어떻게 비밀번호를 조합할지를 신경 쓸 필요가 없고, 문자, 숫자, 기호가 복잡하게 조합된 비밀번호를 외울 필요가 없다.[20] 새로운 비밀번호는 당신의 지문, 음성, 얼굴, 심장박동, 심지어 특징적인 동작과 같은 당신의 일부다. 지문과 홍채, 음성, 안면 인식을 포함해 스마트폰 카메라와 음성 녹음기로 포착할 수 있는 생체인증이 가장 먼저 널리 사용될 것이다. 사용자의 생체인식 데이터를 사용자만이 소유한 신뢰하는 기기로 검증하는—중앙 저장소의 개념과 반대되는—방식이 가장 선호되고 있다. 예를 들어 사용자 스마트폰의 특정 자료에 접근하기 위해 사용자의 지문을 사용하면, 이어서 그 기기의 고유한 서명이 인증 메커니즘에 전송되고 메커니즘은 사용자의 접근을 허용한다.[21] 이것이 다수의 온라인 서비스들에 걸친 인증 확장성의 기본이며 FIDO 협의회가 채택한 모델이다.

리스크 기반 인증의 사례

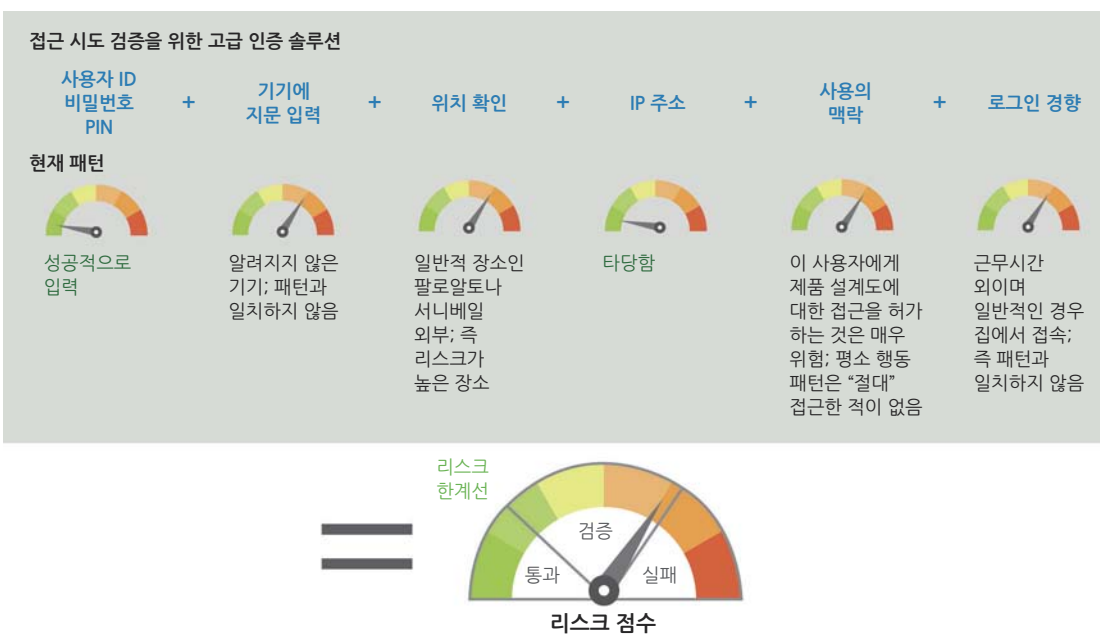
그림 4에 등장하는 가상의 사례를 살펴보자. 한 기업 사용자는 보통 오전 8시30분에 로그인하고 오후 6시쯤 로그아웃 했다가 오후 9시30분 경 다시 로그인 한다. 보통 팔로알토나 서니베일에 있는 회사의 사무실에서 로그인하고 회사의 시스템에는 낮 동안 회사의 노트북이나 데스크톱을 이용해 회사 시스템에 접속한다.

어느 월요일, 이 사용자가 서니베일 사무실에서 오전 11시에 로그인해 회사의 컴퓨터를 사용해 기업의 재무 시스템에 접속하려고 한다. 이 사용자는 회사 사무실에 있는 회사 컴퓨터로 근무 시간에 로그인해 평소에 접근하는 정보를 구하려고 한다. 이 때 시스템은 접속을 승인해준다.

다음 날, 이 사용자는 오후 7시에 로스앤젤레스 국제공항에서 회사의 노트북을 사용해 사내의 복지 시스템에 있는 회사 휴무일 목록에 접속하려고 한다. 비록 그가 있는 장소와 시간이 평소와 다르지만, 그 외 요소들은 전형적인 그 사람의 것이며 그가 찾는 정보는 민감한 것이 아니다. 이때도 시스템은 접속을 승인 해준다.

그 다음 날, 해커가 오전 3시에 벨라루스에서 앞의 사용자의 사용자명과 비밀번호로 내부 개발 서버에 있는 회사의 미출시 제품의 설계도에 접근을 시도한다. 사용자명, 비밀번호, IP 주소는 타당하다. 하지만 다른 요소들, 즉 장소, 시간, 요청 정보 등은 이 사용자에 있어 지극히 이례적이다. 시스템에는 사용자의 신원을 검증하기 위한 단계적 상향 인증 기법을 시행하는 통제절차가 설치되어 있다. 예를 들어 사용자의 휴대전화로 1회용 인증코드를 보내는 것이다. 이 상황에서 해커가 사용자의 전화를 가지고 있지 않기 때문에 인증 코드를 입력할 수 없고 시스템은 접근을 거부한다.

그림 4. 리스크 기반의 사용자 인증 사례



그래픽: Deloitte University Press | DUPress.com

"당신이 가진 것"이란 범주로 또 다른 인증요소들을 묶어서 정의할 수 있다. 스마트폰뿐 아니라 개인이 가지고 다니는 보안 토큰, 소프트웨어 방식의 토큰 혹은 심지어 비트코인이 이용하는 블록체인 데이터베이스의 적용까지 이 범주로 묶을 수 있다. 하드웨어 USB 키는 직원들이 사용자명과 비밀번호를 입력하여 로그인할 때 정해진 시간 간격으로 생성되는 무작위 암호를 추가 입력하는 절차를 가능하게 해준다. 소프트웨어 토큰도 유사하게 동작하는데, 예를 들어 스마트폰 앱을 통해 무작위 암호를 생성한다. 거기에 더해, 분산화된 블록체인 기술의 사용은 인증을 위한 더 안전하고 분권화된 시스템을 제공하는 데 도움을 줄 수 있는 잠재력이 있다.

새로운 접근통제 방법들 중 가장 흥미로운 가능성은 리스크 기반 인증(Risk-based authorization)으로, 허가를 요청하는 사용자의 신뢰성과 보호하고 있는 정보의 민감성에 따라 접근을 허가해주는 역동적인 시스템이다. 구글의 첨단기술프로젝트팀(Advanced Technology and Project)에서 추진하는 프로젝트 아바커스(Project Abacus)는 사용자 행동에 대한 복합적인 평가를 기반으로 사용자를 인증하기 위한 머신러닝을 개발하고 있다.[22] 카메라, 가속도계, GPS 기능과 같은 센서들을 이용해 스마트폰은 사용자에 대한 광범위한 정보를 모을 수 있다. 여기에는 전형적인 얼굴 표정, 습관적인 위치 정보, 타자를 치는 법, 걷는 법, 말하는 법 등이 포함된다. 이를 종합하면, 이들 요소는 지문보다 10배 안전하고 4자리 PIN 번호보다 100배는 안전하다.[23] 이러한 역량을 가지고, 사용자의 전화나 다른 기기는 지속적으로 신뢰 점수, 즉 사용자가 자신이라고 주장하는 사람이 맞는지 확인할 수 있는 신뢰도를 계산할 수 있다. 만약 시스템이 의심을 가지게 되면, 단계적으로 상향되는 인증 절차를 통해 사용자의 신원을 검증하기 위한 더 많은 증거를 요구하거나 접근을 거부한다.

이런 신뢰 점수 기법은 정보의 민감도에 따른 정보 보호를 설계할 때 유용하다. 예를 들어서 은행 앱은 신뢰 점수가 매우 높아야만 하고, 반면 일반적인 뉴스 사이트는 그렇지 않아도 된다. 이러한 접근법이 널리 도입되기 위해서는 회사들이 소비자의 사생활 문제를 고려해야만 한다.

가장 강력한 방어

회사가 어떻게 새로운 시스템을 채택하는지 살펴보기 위해 한 유통 체인이 고객의 신용카드 정보가 도난 당했다는 사실을 발견한 시나리오를 가정해보자. 앞으로의 공격을 방어하기 위해 이 회사는 잠재적인 취약점에 대한 전사적인 평가를 시행했고 공격으로 이어질 수 있는 3가지 취약점들을 발견했다. 첫째, 서버 관리팀이 공유 디렉터리에 암호화하지 않은 텍스트 파일로 사용자명과 비밀번호를 저장했다. 둘째, 편의를 위해 점포 관리자가 POS 단말기의 비밀번호를 직원들과 공유해 이들이 환불이나 교환 등을 할 수 있는 더 높은 권한을 주었던 사례가 드러났다. 마지막으로 통합 업무를 간편하게 하기 위해 외주업체에 발급한 비밀번호가 절대로 만료되지 않도록 설정되어 있었다.

분석 결과에 따르면 이 유통업체는 보안 침해의 원인일 가능성이 가장 큰 판매 시점의 보안을 강화하기 위해 몇 가지 새로운 인증 방식을 고려했다. 관리자는 직원이 시스템에 접근하려고 할 때마다 스마트폰으로 전송된 1회용 비밀번호를 입력하는 대안에는 불편함을 이유로 반대했다. 대신에 점포의 한 부문에서 점포 직원의 POS 시스템 로그인을 인증하기 위해 지문과 안면인식의 조합을 시험해보기로 한다. 이는 사용자에게 편리할 뿐 아니라 기존의 인프라를 활용한다. 이미 POS 활동을 모니터링하기 위해 설치된 카메라와, POS 하드웨어의 터치스크린 로그인 화면에 부착된 지문 스캔 애플리케이션을 사용해, 회사는 추가적인 하드웨어 없이 시범 프로그램을 시작했고 제3자 소프트웨어 개발 비용만을 추가 사용했다. 결과는 다음과 같다. 점포직원들은 쉽고 빠른 로그인을 좋아하게 됐

고 회사는 대상 사용자들에게 적절한 권한을 부여하게 됐다. 그리고 POS 카메라가 항상 지켜보고 있다는 생각이 직원들의 절도 감소에도 공헌했다.

시범 프로그램의 성공으로 이 유통업체는 해당 솔루션을 1,500곳의 전 지점으로 확대했고, 새 시스템의 보안을 보장하기 위해 보안정책도 갱신했는데, 여기에는 더 큰 영향을 미치는 더 중요한 운영업무에도 지문과 안면 인식을 적용하는 것과 손상된 인증 요소를 안전하게 복구하기 위한 메커니즘도 포함된다.

또한 회사는 점포 직원 교육을 시행했다. 현지 점포의 훈련강사는 신규 시스템의 편리함과 과거 사이버 침해의 원인이었던 취약점에 대한 효과성, 그리고 회사가 직원과 고객의 이익을 위해 최신 기술에 투자하고자 하는 의지를 강조했다. 또한 훈련강사는 해당 솔루션의 작동 원리를 설명하는 문서를 공유해, 생체인증 정보가 POS 인증 외에는 사용되지 않을 것임을 확실히 했다.

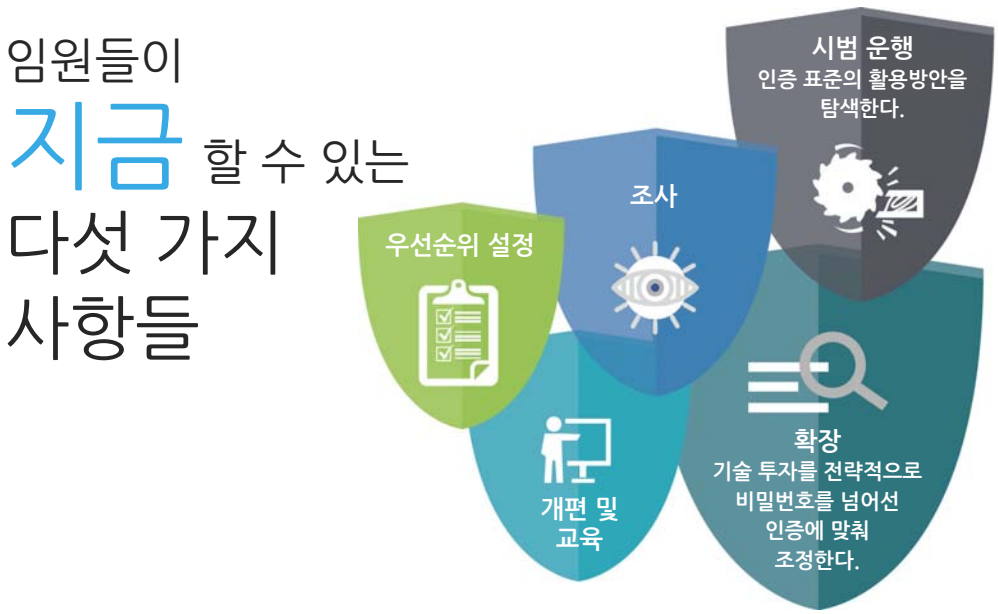
보안뿐만 아니라 디지털 전환으로

비밀번호를 넘어 진화하는 것은 단지 미래의 물결이 아니라, 오늘날에도 경제적 의미가 있다. 미국 기업을 대상으로 최근 실시한 설문조사에 따르면, 비밀번호 관련 문제로 인해 각 직원마다 연간 평균 420달러의 손실이 발생한다고 한다.[24] 조사대상자 중 37%가 연간 50회 이상 비밀번호를 재설정했으며, 그로 인한 생산성 손실은 엄청날 것이다.[25] 필요한 지원팀 직원이나 헬프데스크와 같은 비용을 고려한다면 비밀번호를 없애는 데서 오는 절약은—보안적 장점은 물론이거니와—전환을 더 빠르게 정당화할 수 있을 것이다. 또한, 직원의 일상 업무를 간소화 함으로써 직원의 만족도와 생산성을 개선할 수 있다. 영국의 고객불만접수 부서에 대한 연구에 따르면 프로세스 개선과 직원 태도 및 유지 사이에 상관관계가 있으며, 광범위하게는 심지어 조직의 재무적 성과에도 변수로 작용할 수 있다.[26]

과거의 —익숙하지만 짜증나는—비밀번호 시스템을 버리고 새로운 로그인 방법을 채택하는 일은 분명 관리자, 사용자, 고객에게 힘든 일로 보일 것이다. 그러한 모든 변화는 매우 실질적인 문제를 극복하기 위한 현실적인 투자와 실행 계획을 필요로 한다. 우선, 기술적인 관점에서 어떠한 시스템도 보안이 완벽하지 않다. 스마트폰이나 토큰이 핵심이라면, 분실하거나 도난된 기기가 리스크를 유발할 수 있다. 신용카드 분실의 경우처럼, 사용자는 기기의 제조자나 인증 기관에 연락해 분실을 신고하고 교체를 요청해야 한다. 사기범들은 때로 계정 탈취를 위해서 잃어버린 인증 요소의 복구 기능을 이용한다.[27] 휴대전화도 취약한 고리가 될 수 있다. 무선 통신은 암호화가 되지 않는 경우가 많기 때문에 전송 중에 탈취될 수 있다.[28]

심지어 생체인증 기술도 절대 안전하진 않다. 많은 경우 속이기 어렵지만 그렇다고 속이지 못하는 것은 아니다. 예를 들어 지문은 모형제작용 점토를 사용해 복제할 수 있다.[29] 시스템 설계자는 이러한 잠재적 취약점을 센서에 생기 감지 기능을 추가하거나 생체인증 정보를 적용 방식마다 특화된 형식으로 저장함으로써 대처할 수 있다. 하지만 이러한 기술은 아직 완전히 실행될 준비가 되지 않았다. 둘 다 비즈니스 과정의 변화 없이는 완전한 혜택을 제공할 수 없는 애널리틱스에 기반한 최고의 시스템이 아니다. 예를 들어, 앞서 삽입글 "리스크 기반의 사용자 인증 사례"에서 살펴본 평판 기반의 보안 시스템을 생각해보자. 그 시스템에서 방어 체계는 시스템 접근을 시도하는 사용자 ID만 검사하는 것이 아니라 사용자의 장소, 시간, 행동 패턴, 접근하고자 하는 데이터까지도 검사한다. 이러한 지표들이 일반적이지 않을 때 시스템은 민감한 비즈니스 정보에 대한 접근을 거부한다. 이는 훌륭한 보안 접근법이지만 조직이 자사의 모든 데이터를 알고 통제한다는 가정에 입각한 시스템이다. 기업은 이미 그 정보를 민감하다고 분류하고 접근에 대한 규약을 정해놓았을 때만

그림 5. 임원들이 지금 할 수 있는 다섯 가지 사항들



그래픽: Deloitte University Press | DUPress.com

누군가 민감한 데이터에 접근하려고 시도한다는 사실을 인지할 수 있다.

그러므로 비밀번호를 넘어서는 일은 어렵게 들릴 수 있고, 내부 지식관리 및 다른 비즈니스 절차에 대한 변화뿐 아니라 주요 IT 분야의 고도화도 필요하다. 하지만 조직은 매끄러운 전환을 위해 점진적인 단계(그림 5)를 밟을 수 있다. 다음은 이를 위한 로드맵이다.

- **우선순위 설정.** 위협 환경에 대항해 전략적 비즈니스 우선순위를 평가한다. 중요도에 따라 평가된 핵심 비즈니스 운영 항목에 대한 인증 시스템의 취약점을 파악한다.

- **조사.** 인증을 더 강화하기 위해 가능한 솔루션들을 조사한다. 가장 큰 위협을 보호하는데 있어 장점과 단점을 평가하고, 특정한 작업 환경에서 현실적이고 비용 효과적이며 확장 가능한 답안을 제공할 수 있는 능력을 평가한다. 표준 기반의 인증 소프트웨어 솔루션을 사용하면 신규 인프라 설치에 소요되는 비용을 회피하고 차세대 솔루션으로 통합할 수 있는 기초를 다질 수 있다.

- **시범 운행.** 가능성 높은 솔루션을 선택한 후에는 한 가지 혹은 몇 가지의 높은 우선순위 비즈니스 운영 항목을 대상으로 시범 프로그램을 진행한다. 이들 시범 운행에서 사용자 경험에 대한 데이터와 피드백을 수집한다. 사용자는 쉽고 직관적으로 신규 솔루션을 사용할 수 있는가? 더 쉬운 온라인 접속이 업무를 더 효율적으로 만들었는가? 온라인 접속이 더 강력한 보안을 제공하는 방향으로 더 자주 올바르게 사용되고 있는가? 사용자가 생체인증이나 그들의 행동 규범에 기반한 반응적/동적 솔루션에 대해 사생활 침해 및 기타 우려사항을 제기하는가? 온라인 관리자의 관점에서 신규 시스템을 유지하는 비용은 과거 비밀번호 시스템과 비교해 어떠한가?

- **확장.** 시범운영에서 얻은 교훈을 이용해 우선순위를 기준으로 더 광범위한 핵심 운영항목들에 솔루션을 적용한다.

- **개편 및 교육.** 접근 정책을 갱신한다. 비밀번호 보안에 대한 정책을 요청된 정보의 민감성에 근거한 리스크 기반의 정책으로 교체한다. 사용자에게 과거 기술과 대비되는 장점에 초점을 맞춰 신규 시스템이 어떻게 작동하는지 교육한다.

기술적 진보는 조직들에게 비밀번호를 넘어설 수 있는 기회를 제공하고 있다. 조직들은 특히 사이버 공격이 확산되고 있는 이 시점에서 그러한 기회의 활용을 심각하게 고려해야 한다. 현재의 비밀번호 메커니즘의 열악한 사용자 경험, 비용 증가, 보안 약화를 고려할 때 기업은 새로운 디지털 인증 시스템으로의 이전을 검토해야 한다. 새로운 시스템은 보안 강화와 사용자 경험 개선이라는 두 가지 목표를 충족시킨다.

조직은 서비스형 소프트웨어 플랫폼의 채택, 옴니채널 사용자 관여 계획과 같은 디지털 변환 노력의 일환으로서 비밀번호 기반이 아닌 인증 솔루션에 투자해 그 과정을 시작할 수 있다. 이러한 신규 솔루션 영역은 기업의 더 광범위한 인증 시스템 개선계획을 위한 기반이 될 수 있는데, 여기에는 시간이 걸릴 수 있다. 기존 플랫폼의 제약과 기술적 한계 때문에 아마도 한동안은 비밀번호와 함께 살아가야만 할 수도 있다. 하지만 그렇다고 비밀번호에 기반하지 않은 인증 시스템으로의 통합을 지연시킬 이유는 없다.

DR

마이크 와이어트(Mike Wyatt)*는 딜로이트 & 투쉬 LLP 사이버 리스크 서비스의 매니징 디렉터이며, 딜로이트 자문 사업부를 위한 디지털 및 기업 아이덴티티 솔루션 서비스를 이끌고 있다.*

이판 사이프(Irfan Saif)*는 딜로이트 & 투쉬 LLP 사이버 리스크 서비스의 프린시펄이다. 미국 자문 기술 부문의 리더이며 또한 딜로이트 CIO 프로그램과 사이버 리스크 사업부의 리더이다.*

데이비드 맵가온카(David Mapgaonkar)*는 딜로이트 & 투쉬 LLP 사이버 리스크 서비스의 프린시펄이며 신원과 접근 관리가 전문분야다.*

*본고에 대한 **아비 고엘(Abhi Goel)**, **콜린 수타(Colin Soutar)**, **이안 글레이저(Ian Glazer)**의 공헌에 감사의 말을 전한다.*

Endnotes

1. LaunchKey, *The decentralized authentication and authorization platform for the post-password era*, May 2015, https://launchkey.com/white-paper.
2. For more on the hidden costs of cyberattacks, particularly with regard to intellectual property, see Emily Mossburg, J. Donald Fancher, and John Gelinne, "The hidden costs of an IP breach: Cyber theft and the loss of intellectual property," *Deloitte Review* 19, July 2016, http://dupress.com/articles/loss-of-intellectual-property-ip-breach.
3. Brian X. Chen, "Apps to manage passwords so they are harder to crack than 'password,'" *New York Times*, January 20, 2016, www.nytimes.com/2016/01/21/technology/personaltech/apps-to-manage-passwords-so-they-are-harder-to-crack-than-password.html.
4. Guillaume Desnoës, "How will we manage 200 passwords in 2020?," *ITProPortal*, September 13, 2015, www.itproportal.com/2015/09/13/how-will-we-manage-200-passwords-in-2020/; Steve Cook, "Could biometric give us a world without passwords?," LinkedIn Pulse, September 17, 2015, www.linkedin.com/pulse/could-biometrics-give-us-world-without-passwords-steve-cook.
5. Ian Barker, "84 percent of people support eliminating passwords," *BetaNews*, October 2015, http://betanews.com/2015/08/27/84-percent-of-people-support-eliminating-passwords/.
6. Hossein Bidgolli, editor, *Handbook of Information Security* (Hoboken, NJ: John Wiley & Sons, 2006), p. 434.
7. Ibid, p. 433.

8. RoboForm, "Password security survey results," www.roboform.com/blog/password-security-survey-results, accessed April 5, 2016.

9. Rob Waugh, "What are the alternatives to passwords?," *WeLiveSecurity*, February 5, 2015, www.welivesecurity.com/2015/02/05/alternatives-passwords/.

10. Chris Hoffman, "Why you should use a password manager and how to get started," *How-To Geek*, September 9, 2015, www.howtogeek.com/141500/why-you-should-use-a-password-manager-and-how-to-get-started/.

11. Kim Zetter, "Hacking team's leak helped researchers hunt down a zero-day," *Wired*, January 13, 2016, www.wired.com/2016/01/hacking-team-leak-helps-kaspersky-researchers-find-zero-day-exploit/.

12. RoboForm, "Password security survey results—part 1," http://www.roboform.com/blog/password-security-survey-results, accessed April 21, 2016.

13. Kevin Cunningham, "Password management problems: Employees significantly increasing risk of security breaches," SailPoint, January 29, 2015, http://www.sailpoint.com/blog/2015/01/survey-password-management/.

14. Ibid.

15. Jeremy Quittner, "Why the 'Internet of Things' nabbed $1 billion in VC in 2013," *Inc.*, March 20, 2014, www.inc.com/jeremy-quittner/venture-capital-flows-to-gadget-and-hardware.html; Chris Quintero, "Who invests in hardware startups?," *TechCrunch*, September 12, 2015, http://techcrunch.com/2015/09/12/who-invests-in-hardware-startups/.

16. Ian Glazer, interview with Mike Wyatt, February 10, 2016, in Austin, TX.

17. See David Schatsky and Craig Muraskin, *Beyond bitcoin: Blockchain is coming to disrupt your industry*, Deloitte University Press, December 7, 2015, http://dupress.com/articles/trends-blockchain-bitcoin-security-transparency/.

18. Visa Europe, "Generation Z ready for biometric security to replace passwords," January 12, 2015, www.visaeurope.com/newsroom/news/generation-z-ready-for-biometric-security-to-replace-passwords.

19. FIDO Alliance, "About the FIDO Alliance," https://fidoalliance.org/about/overview/, accessed April 5, 2016.

20. PYMNTS.com, "Is it time to cash in PINs for biometrics?," January 28, 2016, www.pymnts.com/news/biometrics/2016/is-it-time-to-cash-in-pins-for-biometrics/.

21. Mark Hachman, "Microsoft's Windows Hello will let you log in to Windows 10 with your face, finger, or eye," *PCWorld*, March 17, 2015, www.pcworld.com/article/2898092/microsofts-windows-hello-will-let-you-log-in-to-windows-10-with-your-face-finger-or-eye.html; Hachman, "Hands on: Without apps, Intel's RealSense camera is a puzzle," *PCWorld*, March 5, 2015, www.pcworld.com/article/2893270/hands-on-without-apps-intels-realsense-camera-is-a-puzzle.html.

22. Beverly Zena Janelinao, "Project Abacus: Google's plan to get rid of the password," *Travelers Today*, January 25, 2016, www.travelerstoday.com/articles/21353/20160125/project-abacus-google-s-plan-to-get-rid-of-the-password.htm.

23. Tom Maxwell, "Smart Lock Passwords is cool, but Google Project Abacus puts us closer to a password-free world," 9to5Google, May 29, 2015, http://9to5google.com/2015/05/29/smart-lock-passwords-is-cool-but-google-project-abacus-wants-to-eliminate-password-authentication/.

24. Centrify, "U.S. businesses lose more than $200,000 annually from employees struggling with passwords," October 14, 2014, www.centrify.com/about-us/news/press-releases/2014/us-businesses-lose-more-than-200-000-annually-from-employees-struggling-with-passwords/.

25. Ibid.

26. Robert Johnston, "Linking complaint management to profit." *International Journal of Service Industry Management* 12, no. 1 (2001): pp. 60–69 (2001).

27. Maya Kamath, "Hackers are using password recovery scam to trick victims into handing over their email account access," *TechWorm*, June 21, 2015, www.techworm.net/2015/06/hackers-are-using-password-recovery-scam-to-trick-victims-into-handing-over-their-email-account-access.html.

28. IBM MaaS60, *Mobile: The new hackers' playground,* Data Breach Today, February 6, 2016, www.databreachtoday.com/whitepapers/mobile-new-hackers-playground-w-2243.

29. Archibald Preuschat, "Watch out, your fingerprint can be spoofed, too," *Wall Street Journal*, February 24 2016, http://blogs.wsj.com/digits/2016/02/24/watch-out-your-fingerprint-can-be-spoofed-too/?mod=ST1