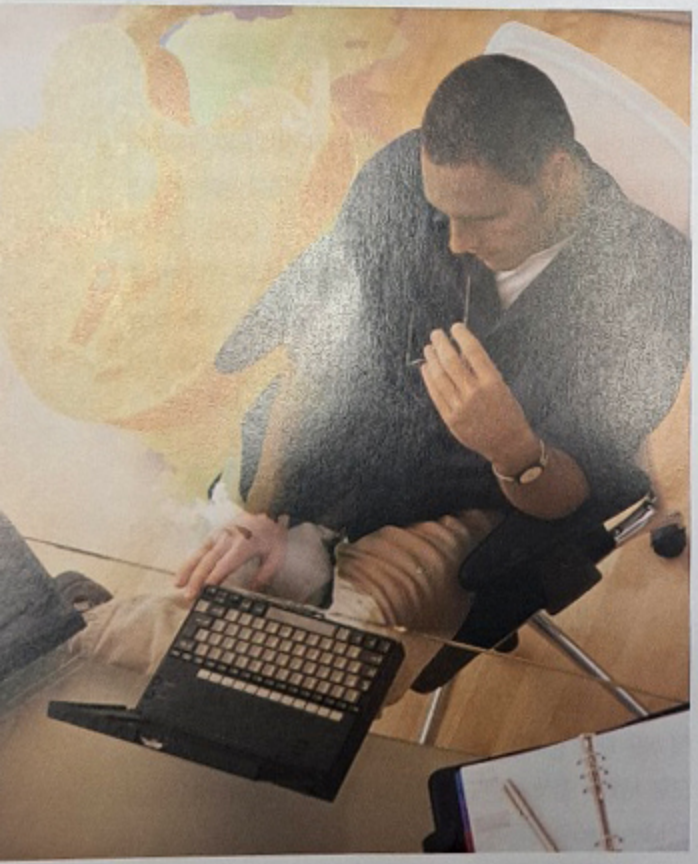
편의성·보안성 보장된 인증 기술로 디지털 ID 보호

인증 시스템 중단은 비즈니스 중단 … 간편하지만 강력한 인증으로 제로 트러스트 이행

인증은 디지털 비즈니스의 관문으로, 인증 시스템이 작동하지 않으면 업무가 중단되고 비즈니스 이행이 어려워진다. 디지털 혁신으로 비즈니스 영역이 넓어지면서 인증이 필요한 업무는 더 많아졌으며, 이로 인한 사고도 늘어났다. 특히 급증하는 디지털 ID의 유효성과 권한을 검증하기 위해 고도화된 인증 기술이 요구된다. 디지털ID의 특징과 차세대 인증 기술에 대해 알아본다. <김선애 기자·iyamm@datanet.co.kr>



사상 초유의 행정망 마비 사고는 새올행정시스템 접속을 위한 GPKI 인증 시스템 장애로 시작됐다. GPKI 서버 연결을 위한 라우터 모듈 포트 일부 이상으로 이 같은 대규모 사고가 일어나면서 디지털플랫폼 정부 진행이 원활하게 이뤄질지 우려하는 목소리가 높아졌다.

액티브 디렉토리(AD) 등 ID 관리 시스템에서 장애가 발생해 업무가 중단되는 사고는 이미 여러 차례 보고됐다. 2020년 마이크로소프트가 정전 정전사고를 당해 마이크로소프트 아이덴티티와 접근관리 서비스가 일시적으로 중단돼 AD 이용 고객들이 업무를 할 수 없었다. 랜섬웨어 공격자들은 기업에 구축된 AD 서버를 인질로 잡기도 한다.

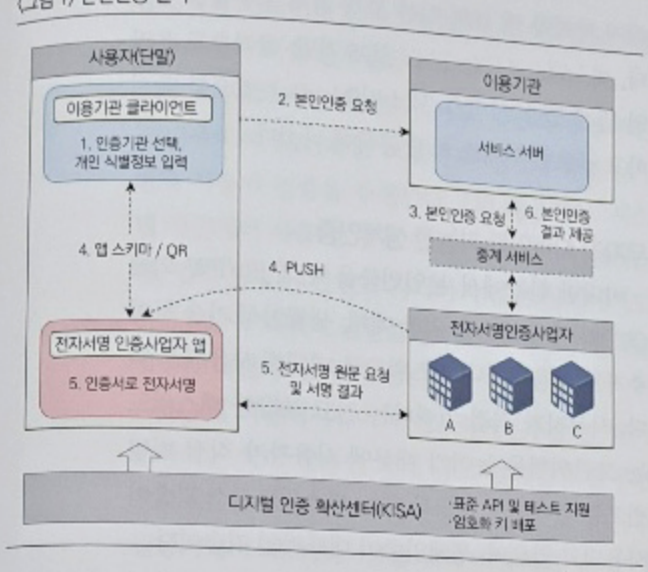
행정망 마비 역시 비슷한 사고로, GPKI 인증서버 장애로 공무원들이 인증을 받지 못해 업무에 접속하지 못했고, 결과적으로 모든 업무 중단으로 이어지게 됐다. 인증이 마비되면 비즈니스가 중단된다는 사실을 보여준 사고라고 할 수 있다.

디지털 비즈니스 관문 '인증'

인증은 디지털 환경에서 가장 먼저 수행되어야 하는 프로세스다. 비대면 디지털 환경에서는 자신이 직접 허가된 서비스에 접근한다는 사실을 입증하는 인증(Authentication)과 본인 자신임을 확인하고 접속을 허락하는 인가(Authorization)를 거쳐야 한다. 사람 뿐만 아니라 기계, 봇, 애플리케이션 등의 접속도 인증, 인가 조치가 필요하며, 이 경우 별도의 행위 없이 자동으로 인증 대상을 확인하고 인가할 수 있어야 한다.

인증과 인가에 문제가 생기면 서비스 접속이 차단되므로 업무가 불가능하다. 그래서 인증과 인가 시스템은 접속 요청에 대해 빠르게 판단하고 허용-차단을 결정해야 하며, 그 과정은 복잡하지 않고 단순해야 한다. 동시에 권

〈그림 1〉 간편인증 절차



(자료: KISA)

한있는 사람과 기기가 권한 내에서, 정상적인 업무 수행 활동만 허가할 수 있도록 설정해야 한다. 그리고 시스템 내에서 일어나는 일련의 행위는 기록으로 남겨야 하며, 중요한 결정을 내릴 때는 권한있는 본인이 직접 결정했다는 사실을 입증하는 전자서명을 해야 한다.

공공·금융 서비스에서 사용하는 공인인증서(현 공동인증서)는 인증서 하나로 본인인증과 부인방지까지 가능했지만, 특정 기술에 종속된다는 비판을 받아 현재는 금융인증서와 다양한 사설인증서가 함께 사용되고 있다.

사설인증서는 스마트폰 앱을 통해 간편하게 인증할 수 있어 사용 편의성이 높지만, 이를 적용한 사업자(이용기관)는 개별 전자서명인증사업자마다 상이한 간편인증 인터페이스를 맞춰야 해 개발과 운영이 복잡하고 중복투자로 인한 비효율성도 높은 상황이다.

이에 한국인터넷진흥원은 '간편인증 인터페이스 가이드라인'을 공개하고 이용기관이 다양한 전자서명수단을 쉽게 도입·상호연동할 수 있도록 돕고 있다. 이 가이드라인에서는 ▲전자서명인증사업자의 간편인증 서비스 제공을 위한 공통 인터페이스 ▲공통 인터페이스 사용을 위한 이해당사자 간의 통신·인증 방법 ▲이용기관 서비스에서 전자서명인증사업자의 인증앱 호출 방법 ▲간편인증 서비스 통신구간의 안전성 확보 방법 등을 안내하고 있다.

PKI 기반 간편인증·통합 플랫폼 제공

국내 PKI 기술을 가진 기업들은 간편인증 서비스 구축·운영에 어려움을 겪는 기업을 지원하기 위한 통합인증 플랫폼을 제공하고 있다. 통합인증 플랫폼은 사업자들이 개별 전자서명인증사업자가 요구하는 환경에 맞게 인증 플랫폼을 구축, 지원해 시간과 비용을 줄이면서 고객 경험을 개선할 수 있게 한다.

이 플랫폼은 대 고객 서비스 뿐만 아니라 내부통제를 위해서도 사용할 수 있다. 최근 인증 시장에서는 소비자 뿐만 아니라 임직원, 파트너사 직원, 서비스에 연결되는 애플리케이션, IoT 기기 등도 '고객'의 범주로 인식하고 있다. 통합인증 플랫폼은 고객의 인증과 서비스 이용을 원활하게 도울 수 있는 간편인증 시스템을 연결하고 있다.

신동규 유넷시스템 보안연구소장은 "PKI는 확실한 법적 효력과 부인방지 기능을 제공하는 안전한 인증으로, FIDO, 매터 등도 기반기술이나 원천기술은 PKI에서 가져왔다"며 "강력한 신원확인과 인증, 데이터 무결성 보장, 데이터 암호화와 안전한 통신, 전자서명과 디지털 문서화, 접근제어와 권한관리, 클라우드·IoT 보안 강화 등 다양한 분야에서 여전히 탁월한 기술로 사용되고 있다"고 말했다.

유넷시스템의 PKI 솔루션과 서비스는 다양한 분야에서 활용되고 있다. 제로 트러스트 내 신원확인, 액세스 제어·권한관리, FIDO·생체인증 연동 시 MFA·패스워드리스 인증으로 활용 가능하며, 서버-클라이언트 인증, 암호화 통신과 인증서 갱신 및 관리 등에 사용된다. 향후 로봇이나 차량 등의 기기간 인증, 기기-인터넷 인증, 소프트웨어 업데이트 및 인증, 기타 인프라 보안 등 인증이 필요한 모든 인프라에 사용될 수 있다.

신동규 소장은 "PKI는 기술 개발 후 현재까지, 그

리고 앞으로 우리가 살아갈 모든 시스템에서 중요한 역할을 할 디지털ID 기술이다. 암호·보안기술에서 '인프라스트럭처'가 포함된 기술이 PKI외에는 없을 만큼 PKI는 안전성이 충분히 입증됐다. 간편인증, 사설인증에도 PKI가 사용되고 있으며, 앞으로 더 다양한 분야에서 활용될 것"이라고 말했다.

결제·인증 통합 솔루션으로 고객 신뢰 제고

편리하지만 강력한 인증을 원하는 추세에 따라 최근 인증은 대체로 스마트폰을 이용하고 있다. 스마트폰으로 본인인증을 하면 연동된 웹서비스 인증이 이뤄지는 방식이다. 금융거래 시, 안면인식으로 본인인증을 한다면, 스마트폰 화면을 바라보는 것만으로도 금융앱 로그인과 이체 확인이 이뤄지는 방식이다.

본인명의 스마트폰을 갖고 있지 않은 사람은 이 방식의 본인인증이 불가능하다. 국내 사용자의 경우, 계좌에 1원을 입금하면서 입금자명을 확인하는 방식, 혹은 신용카드 정보를 이용해 스마트폰 인증을 대신하지만, 국내 거래 계좌나 신용카드가 없으면 불가능하다.

이를 대체하는 방법으로 이메일, SNS에 인증을 위한 일회용 비밀번호나 본인인증 링크를 이용하지만, 보안에 취약하다는 문제가 있다.

국내 본인명의 스마트폰, 은행계좌, 신용카드가 없는 해외 거주 교민을 위한 알뜰폰 상품이 있지만, 사용 빈도가 낮은 '본인인증'만을 위해 스마트폰 사용료를 지불하는 것은 부담스럽다. 이 문제를 해결하기 위해 재외동포청은 전자여권을 이용해 인증서를 발급할 수 있도록 지원하고 있다. 재외동포청은 한국인터넷진흥원과 재외동포 비대면 신원확인 법·제도 마련과 비대면 신원확인의 안정성·신뢰성 제고 등을 위해 협력하고 있다.

이 사업에 인증 기술을 제공하고 있는 넥스원소프트는 결제·인증을 통합한 독자적인 기술을 제공한다. 사설인증 사업자, 분산ID 등 인증이 필요한 여러 서비스에 대한 통합인증을 지원하며, 인증부터 결제까지 체계화 해 10% 이상 고객 결제 성공률을 높인다. 넥스원소프트는 EMV 3DS 기반 '클라우드 온라인 결제 인증 서비스 '넥스비(NexBe) 3DS'를 출시하고 글로벌 서비스 시장 공략에 나섰다.

무자각 지속인증 가능한 생체인증

비대면 환경에서 본인인증을 위해 ID/PW 외에 OTP와 기타 인증을 위한 매체, 생체인식 기술 등이 추가로 사용되거나 패스워드를 대체해 사용되고 있다. 사용자가 직접 입력하는 길고 복잡한 패스워드는 보안위협을 높이기 때문에 사용자가 직접 비밀번호를 관리하지 않도록 하는 패스워드리스 기술이 사용되고 있으며, 생체인증이 대표적인 기술이다.

생체인증은 무자각 지속인증을 실현할 수 있어 제로 트러스트를 위한 최적의 인증기술이라고 할 수 있다. 제로 트러스트는 지속적으로 신뢰를 평가해야 하는데, 실제 서비스에 적용했을 때 사용자를 불편하게 해서는 안된다.

사용자의 키보드 타이핑 습관을 인식해 본인 여부를 지속적으로 판단하는 기술이 고려된 적이 있지만, 이 기술은 정확도가 떨어져 상용화되지 못했으며, 최근에는 악성봇 방지에 적용돼 자동화된 봇에 의한 접근인지 사람에 의한 접근인지 구분하는데 사용되고 있다.

무자각 지속인증을 가장 쉽게 이행할 수 있는 방법은 안면인식 기술이다. PC나 스마트폰 화면을 바라보고 있는 것만으로도 인증을 수행할 수 있기 때문에 인증을 위해 별도의 행위를 하지 않아도 된다. 행위가 실시간으로 기록되기 때문에 문제가 생겼을 때 조사 자료로 사용될 수 있으며, 부인방지 기능도 할 수 있다.

피앤피시큐어는 비전 AI 기술을 적용한 안면인식 기술 '페이스락커(FaceLocker)'를 인증이 필요한 모든 업무에 적용해 무자각 지속인증을 통한 제로 트러스트를 구현하고 있다. 페이스락커는 웹캠이 장착된 스크린을 바라보면서 업무를 하면 지속적인 인증이 가능하다. 윈도우 로그인, 기업 계정 시스템

등에 1차 인증수단으로 사용할 수 있게 해 보안은 강화하면서 사용 편의성은 높였다.

피앤피시큐어는 페이스락커를 접근제어 솔루션 '디비세이퍼(DBSAFE)' 제품군과 연계해 작업 단계별로 사용자 검증을 수행한다. DB 접근제어, 시스템 접근제어 사용 중 중요·금지 명령어를 실행했을 때, 업무 담당자 본인이 자각하지 않은 상태에서도 본인인증이 이뤄져 권한을 탈취한 공격자가 임의로 명령을 내릴 수 없게 한다.

류승열 피앤피시큐어 페이스락커본부장은 "페이스락커는 국내 금융권 최대 규모 안면인증 솔루션 프로젝트를 수행하면서 안전성이 검증됐으며, 다수 금융사에서 재택근무 등을 위해 사용하고 있다. 사용자 인증 외에도 이상행위 탐지 업무화면 차단, 카메라 등 객체 탐지 기능을 제공해 강력하고 편리한 본인인증과 부인방지 기능을 제공할 수 있다"고 말했다.

FIDO 기반 간편인증으로 서비스 확장력 높여

패스워드리스 인증 기술 대부분 FIDO 표준을 따른다. FIDO 표준이 제정됐기 때문에 생체인증과 같은 편리하고 강력한 간편인증을 이용할 수 있게 됐다. FIDO는 사용자 기기의 안전한 저장소에 크리덴셜과 시크릿 정보를 저장하고, 필요 시 사용자 본인이 이를 활용해 본인임을 입증하면 연계된 웹서비스 로그인과 거래 인증을 할 수 있다. 모바일 뱅킹 이용 시 로그인과 이체 비밀번호 입력 대신 스마트폰의 안면인식 기능을 이용하는 것을 예로 들 수 있다.

FIDO 기반 간편인증 서비스 중 와이키키소프트의 '와이덴티티(Ydentity)'가 시장의 주목을 받고 있다. 와이키키는 안랩의 전략적 투자를 받아 안랩 임직원용 인증 시스템과 트러스가드 VPN 인증 및 기타 안랩 제품에 와이덴티티 활용 생체인증을 탑재했다. 더존비즈온 차세대 UC에도 탑재해 별도 연동 없이 라이선스 활성화만으로 생체인증이 가능하도록 했다.

조한구 와이키키 대표는 "와이키키는 FIDO 기반 인증의 원천기술을 갖고 있으며, 여러 기업과 기관에 간편인증 시스템을 성공적으로 구축해왔다. 앞으로 인증 수단과 정책, 모니터링까지 아우르는 인증 라이프사이클 관리를 일원화하고, AI 기술을 접목한 진화된 솔루션으로 국내와 글로벌 시장 공략에 나설 것"이라고 밝혔다.

안전한 스마트홈 위한 매터 표준 지원

인증은 사람 뿐만 아니라 사물에도 필요하다. IoT가 늘어나면서 연결되는 기기간, 기기와 네트워크 간 인증이 필요한데, 이 경우 사람의 개입이 불가능하기 때문에 자동으로 인증과 인가가 가능한 인증 플랫폼이 필요하다.

우리나라에서는 월패드 해킹 사고 후 홈네트워크 보안과 스마트홈 보안에 대한 관심이 높아졌으며, 국내 주요 가전 제조사들이 스마트홈 기기의 인증 표준인 '매터(Matter)' 지원 제품을 내놓기 시작하면서 이 시장도 성장을 예고하고 있다.

디지서트의 경우 매터 루트 인증기관으로서, 스마트홈 제조사의 신속한 시장 출시를 지원한다고 강조하면서 자사 경쟁력을 강조한다. 디지서트는 'IoT 트러스트 매니저(ITM)'를 통해 매터 기기 인증서 검색, 보고, 인증 생성과 취소, 사용자 접근·허가 등을 중앙집중 관리할 수 있게 한다.

한번의 클릭으로 기기 신원 인증, 암호화 및 무결성 작업을 간단히 수행할 수 있으며, 기기 데이터 시각화를 암호화, 제조·공장 프로세스 데이터와 결합해 기기 전반에 대한 가시성을 제공한다. 디바이스 전체 수명주기의 보안 관리를 처리할 수 있으며, 현장의 기기에 설치된 펌웨어의 무선(OTA) 업데이트에 대한 보안도 관리할 수 있다.

디지서트는 '디지털 흔적(Digital Footprint)'을 안전하게 관리할 수 있는 다양한 솔루션을 제공하는 기업으로, 특히 SSL/TLS 인증서 '서트센트럴(CertCentral)'은 이 시장 최대 점유율을 갖고 있다. 서트센트럴은 유연한 자동화 옵션을 제공해 배포 규모에 상관없이 인증서 구매, 설치, 모니터링, 검

사, 갱신 및 복원과 같은 주요 관리 작업의 자동화를 지원한다.

디지서트는 다양한 종류의 디지털 신뢰 제품을 '디지서트 원(DigiCert ONE)'이라는 단일 플랫폼에서 제공한다. 이 플랫폼에서 제공하는 기능 중 '트러스트 라이프사이클 매니저(TLM)'가 있는데, TLM은 기업 인증서의 중앙화된 가시성과 제어 기능을 제공하는 솔루션이다. 최근 구글을 중심으로 SSL/TLS 인증서 수명을 90일로 단축시키는 것에 대한 논의가 진행되고 있는데, 인증서 관리를 위해서는 TLM과 같은 솔루션이 필수로 요구될 것으로 보인다.

인증서 생명주기 관리로 신뢰할 수 있는 웹 운영

SSL/TLS 인증서는 신뢰할 수 있는 기업·기관이 운영하는 웹사이트로, 개인정보 등 민감정보가 안전하게 보호되고 있다는 사실을 증명하는 것이다. 인증서가 제대로 작동하지 않거나 만료됐을 때 웹 서비스가 정상 작동하지 않는 불상사가 생긴다. 우리나라에서도 카드사에서 만료된 인증서를 갱신하지 않아 서비스가 중단되는 대규모 사고가 발생한 바 있다.

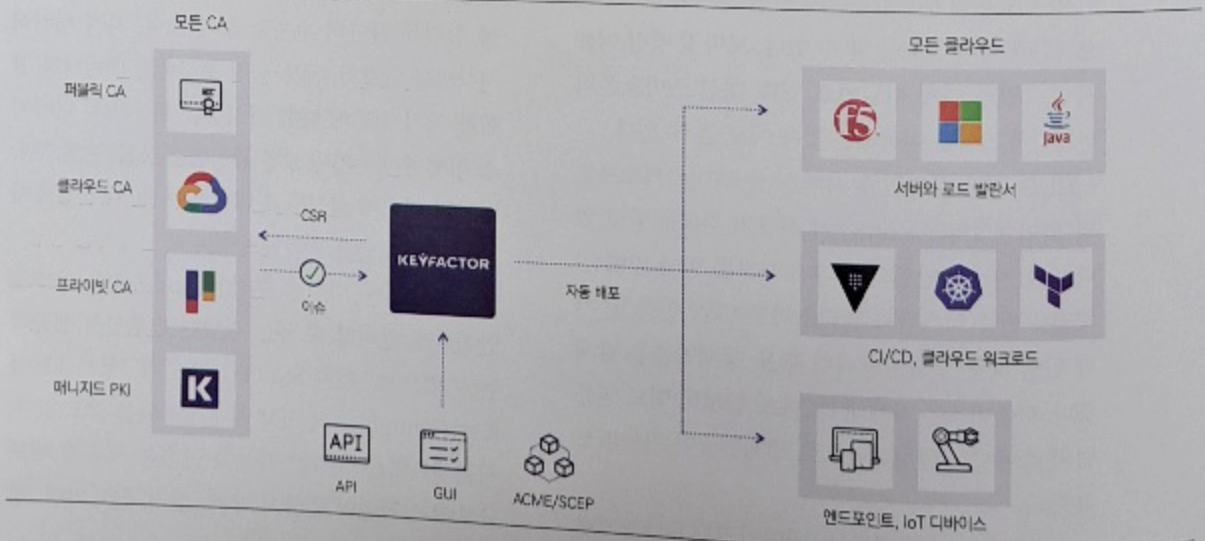
진네트워크가 국내에 공급하는 키팩터의 인증서 생명주기 관리(CLM) 솔루션 '커맨드(Command)'는 쉬운 구축, 편리한 관리환경을 장점으로 시장 공략에 나선다. 인증서 관리에 대한 전문지식이 없는 중소 온라인 쇼핑몰, 웹 기반 서비스 사업자, 소프트웨어 전자서명, 병·의원 진료기록 등 다양한 분야에서 수요가 발생할 것으로 예상하고 있다.

박종필 진네트워크 상무는 "디지털 트랜스포메이션으로 인해 비즈니스가 웹을 중심으로 운영되고 있다. 이로 인해 기업이 관리해야 할 SSL/TLS 인증서가 크게 늘어나게 될 것이며, 인증서 유효기간 단축으로 인한 자동화 관리 요구가 증가할 것"이라며 "키팩터 솔루션은 CA와 모든 클라우드를 위한 단일 플랫폼으로, 셀프서비스와 자동화, 데브옵스 통합 등의 편의 기능을 제공하면서 경쟁력을 높이고 있다. 국내 기업들에게도 CLM의 필요성과 키팩터 장점을 알리면서 시장 공략에 나선 것"이라고 말했다.

IoT 위한 강력 인증 제공

IoT 인증과 관련된 기술 이슈 중에는 IoT를 관리하는 사람과 기기의 인증 문제를 해결하는 것이 시급한 과제로 꼽히고 있다. 대규모 IoT 기기를 관리하는 소수의 관리자들이 ID/PW를 공유하면서 많은 보안문제가 불거지고 있다. 대표적인 예로

〈그림 2〉 키팩터 커맨드 구성도



CCTV 관리자 계정을 별도로 설정하지 않거나 공유 계정을 사용해 계정 해킹으로 사생활과 기밀정보가 유출되는 사례를 들 수 있다.

국내에서는 CCTV 비밀번호 관리를 의무화하는 규제가 있으며, 휴네시온, 한싹, 파이오링크 등 보안기업들이 비밀번호 관리 솔루션을 공급하면서 시장을 성장시키고 있다. 이 솔루션은 개별 CCTV와 NVR의 계정과 비밀번호를 대신 관리하며, 관리자는 계정과 비밀번호를 알 필요 없이 본인 인증만으로 대규모 CCTV를 관리할 수 있게 한다.

센스톤의 경우 OT 환경에서 사용되는 PLC에 대한 ID/PW 관리는 일회용 인증코드(OTAC)로 대신하거나 2차인증으로 사용할 수 있게 한다. PLC 역시 소수의 관리자가 개별 PLC를 일일이 관리할 수 없어 동일한 ID/PW를 사용하거나 관리자들끼리 계정 정보를 공유한다. 이로 인해 생기는 문제를 해결할 수 있도록 매번 바뀌는 일회용 인증코드를 통해 인증하도록 한다.

센스톤 OTAC는 하드웨어와 네트워크 환경을 그대로 유지한 상태에서 사용자 인증을 강화할 수 있어 인증 시스템을 교체하지 않고 운영 가능하다. LS일렉트릭이 생산하는 PLC의 보안을 강화하기 위해 OTAC를 적용했으며, 다른 글로벌 제조사도 적용을 검토하고 있다.

센스톤은 OTAC 기술을 일회용 가상 신용카드 번호, 드론 제어, 인도네시아 조폐공사 전자수입인지 위변조 방지 등에 적용해 상용화했으며, SDK로도 제공해 인증이 필요한 모든 서비스에 적용하고 있다. 또한 신용카드와 스마트폰을 가까이 댔을 때 인증이 되는 카드태깅방식 인증 서비스도 지원해 스마트폰 해킹, 악성앱으로 인한 전자금융사기 사고를 막을 수 있게 한다.

유창훈 센스톤 대표는 "스마트폰 악성앱을 이용해 피해자의 개인정보와 신용카드 정보를 모두 입수한 공격자가 피해자 계좌에서 무단으로 돈을 인출하거나 대출을 받고, 신용카드를 결제하고 있는데, 금융사 입장에서는 모두 다 정상적인 본인인증을 거친 후 진행되는 거래이기 때문에 FDS로 막지 못했다. 이 같은 피해를 막기 위해서는 물리적인 매체를 이용한 인증이 필요하다. 사용자들이 항상 소지하는 스마트폰과 신용카드를 인증 매체로 사용한다면 악성앱을 통한 사고는 막을 수 있다"며 "센스톤은 전자금융사고 방지를 비롯해 모든 인증과 관련된 위협을 사전에 방지할 수 있는 OTAC로 디지털 환경과 OT·IoT 모두를 보호할 수 있게 한다"고 말했다.

탈취한 계정정보, 다른 공격에 이용

안전한 사용자와 기기 인증 기술은 사용자 계정이 탈취돼 공격자가 정상 계정 정보를 이용해 접근을 시도하는 것도 막을 수 있다. 그런데 인증에 필요한 정보까지 모두 공격자가 입수한다면 아무리 강력한 인증도 소용없게 된다.

MFA 피로공격의 경우, 공격자가 일부러 잘못된 MFA 정보를 입력해 사용자가 실수로, 혹은 귀찮아서 MFA 설정 초기화 확인 버튼을 누르게 한 후, 공격자 정보로 MFA를 등록한다.

MFA 설정이 되지 않은 휴면계정에 MFA를 무단으로 등록한 후 정상 권한계정 사용자로 위장하거나, 사용자 정보를 미리 입수한 공격자가 MFA 발급 조직에 직접 연락해 MFA를 재설정한다. 글로벌 기업은 시차를 이용해 공격하기 쉬운데, 피해자가 자고 있는 시간에 MFA를 재설정하거나 비행기를 이용해 이동중일 때, 기타 연락이 어려울 때 MFA를 재설정해 잠입하고 공격을 진행한다.

공격자는 피해자의 계정과 개인정보를 미리 입수해 이러한 공격을 진행한다. 반복되는 개인정보 유출 사고로 개인정보는 공공재나 마찬가지인 상황이 됐기 때문이다. 공격자는 이미 유출된 계정정보를 무작위로 입력해 로그인하는 크리덴셜 스터핑 공격으로 초기 침투를 달성하고 있다. 초기 침투만 전문으로 하는 IAB의 경우, 가장 시간이 많이 드는 계정 탈취와 권한 획득 후 시스템 잠입에 성공한 후 대행 수수료를 받는다.

이러한 공격을 개시할 때 첫번째로 필요한 계정 정보 탈취를 위한 공격은 상시 진행된다. ID 관리 기업 옥타가 연이어 해킹당해 고객정보를 탈취당하고 있는데, 이로 인해 옥타를 이용하는 전 세계 1만 8000여 기업·기관이 영향을 받을 수 있다.

가장 쉽게 계정을 탈취하는 방법은 이메일, SNS 등을 이용해 사회공학 기법으로 접근하는 피싱이다. 이력서, 급여이체 확인증, 연말정산 증빙서류 등 업무 혹은 일상생활과 관련된 메일을 보내 피해자를 감염시키고 정보를 탈취한다.

글로벌 호텔 체인 MGM 리조트가 대규모 해킹피해를 입었는데, 공격자는 링크드인을 통해 관리 직원 정보를 입수한 후 헬프 데스크에 전화해 이 직원의 인증정보를 바꾸고 공격을 진행했다.

대규모 디지털 ID 성공운영 사례로 글로벌 진출

계정탈취 공격차단을 위해 계정 소유자의 각별한 주의가 필요하지만, 소유자가 아무리 주의한다 해도 집요하고 지속적으로 시도하는 공격에 완벽하게 대응하지는 못한다. 그래서 디지털 ID를 관리하는 새로운 방법으로 분산ID(DID)가 제안된다. 블록체인 네트워크에 디지털 인증서를 등록하고, 이 네트워크에 참여하는 기업이라면 별도의 회원가입과 개인정보 제공 없이 등록된 ID로 로그인 할 수 있도록 하는 방식이다.

라온시큐어가 DID 시장을 적극 공략하고 있으며, 행정안전부 모바일 신분증 서비스에 플랫폼을 제공하면서 안정성을 입증했다. 라온시큐어는 FIDO 얼라이언스 보드멤버로, 이 협회를 글로벌 연합체로 성장시켜왔다.

이 경쟁력을 기반으로 설계된 라온시큐어 '옴니원 디지털 ID'는 디지털 증명서, 디지털 배지, 각종 증명서, 자격증, 이수증 발급과 관리, 사물인증(IDoT) 등에 사용할 수 있다. 세종시 블록체인 기반 자율주행차 신뢰 플랫폼 구축 사업을 성공시킨 바 있으며, 향후 스마트팩토리, 디지털 헬스케어, 발전소, 스마트시티, 교통 인프라, 스마트홈, 웨어러블 디바이스 등 다양한 분야에 적용할 수 있다.

라온시큐어 관계자는 "전 세계 13억 인구가 신분증이 없어 국가 복지 체계 혜택 등에서 소외 되고 있다. 이 국가는 디지털 ID 도입이 필요해 월드뱅크, UN 등이 지원하고 있다. 라온시큐어는 행안부 모바일 신분증 등 대규모 디지털 ID 발급·운영 성공 사례를 갖고 있어 글로벌 도전에 유리한 조건을 갖고 있다"며 "라온시큐어는 인도네시아와 동남아시아, 남미 다수국가와 디지털 ID 도입을 논의하고 있다"고 말했다.

계정 관련 거버넌스로 서비스 보호

디지털 환경에서 '계정(Identity)'은 로그인 시 필요한 ID 정보에만 국한되지 않는다. 사람, 사물, 봇, 애플리케이션, 데브옵스 등 연결되는 모든 것에 부여되며, 신원정보, 특성, 권한 등 다양한 정보가 포함된다.

세일포인트 조사에 따르면 조직 내 아이덴티티의 30% 이상이 기존 아이덴티티 솔루션 관리 범위 밖에 있으며, 특히 외주·협력사, 비 인간 아이덴티티, 데이터가 취약한 것으로 나타났다. 또 기업이 활용하는 IT 리소스가 늘어나면서 사용자 정보, 속성, 자격 증명까지 무분별하게 폭증하는 '아이덴티티 스프롤(Identity Sprawl)' 현상도 일어난다. 세일포인트는 비인간 아이덴티티가 3~5년간 가파르게 증가할 것으로 예상하면서 더 심각한 보안문제가 발생할 것이라고 내다봤다.

세일포인트는 아이덴티티 거버넌스 관리(IGA) 솔루션 기업으로, 아이덴티티 관리·보안과 관련된 솔루션을 단일 플랫폼에서 제공한다. 회사 임직원과 외부 파트너, 비인간 계정까지 포괄하는 아이덴티티와 액세스 가시성을 확보·통제할 수 있으며, 다양한 워크플로우·시스템과 통합돼 아이덴티티와 사용권한 전반의 인사이트를 제공한다. AI/ML 기반 인텔리전스를 통해 아이덴티티·권한 소유와 사용에 대한 비정상적 패턴을 감지해 알려준다.

세일포인트는 국내 대형 제약사에 성공적으로 플

랫폼을 구축해 디바이스, 장비, 제조시설과 연동된 아이덴티티·권한관리를 제공했다. 또 금융 클라우드 규제 개선과 함께 개화되는 금융 클라우드를 위한 아이덴티티 솔루션 시장에서도 경쟁우위를 다지기 위해 금융시장 공략에도 속도를 내고 있다.

지정권 세일포인트코리아 지사장은 "세일포인트는 민첩성과 혁신성이 뛰어난 아이덴티티 솔루션을 제공한다. 데이터 사이언스 전담팀이 높은 수준의 AI를 적용해 엔터프라이즈 고객이 필요로 하는 지능적이고 자율적인 대응이 가능한 아이덴티티 보안 방식을 제공할 수 있다"며 "국내 제조, 금융권에서 세일포인트의 강점을 인정하고 높은 관심을 보이고 있어 높은 성장이 가능하다고 자신한다"고 말했다.

권한계정 보호해 심각한 위협 사전 방어

계정에는 권한이 부여된다. 공격자가 이용하는 것은 '권한'이며, 높은 권한을 가진 계정일수록 공격당하기 쉽다. 사이버아크 조사에 따르면 민감도가 높은 직원의 접근성이 적절하게 보장되지 않고 있다고 답한 IT 전문가가 62%에 이르며, 인간보다 더 많은 수의 머신이 민감한 액세스 권한을 갖고 있다고 응답했다(39% 대 45%).

가장 민감한 권한계정은 가장 강력하게 통제되어야 하는데, 실제 현장에서는 아웃소싱 직원에게도 최고관리자 권한을 부여하는 등 기본적인 관리조차 되고 있지 않다. 그래서 권한접근관리(PAM) 솔루션이 필요하다.

PAM은 권한을 가진 모든 계정을 관리·보호해 권한탈취 공격자의 이상행위를 막을 수 있다. PAM은 제로 트러스트 원칙에 따라 최소한의 범위에서만 권한을 부여하고 지속적으로 신뢰를 평가해 이상행위를 탐지하고 권한 사용자의 오남용을 막을 수 있게 한다.

PAM 분야 리더인 사이버아크는 시스템, 애플리케이션, 엔드포인트, SaaS 전반에서 권한있는 계정을 관리하면서 감염된 기기와 사용자의 권한을 즉시 제한하고 차단해 전체 인프라를 보호한다. 인사 시스템과 연동해 디지털 ID, 애플리케이션, 업무 시스템, 시스템 권한 일관성을 신속하게 관리하고 정확하게 운영할 수 있다. 사이버아크 통합인증 플랫폼은 국내 제조, 이커머스, 제약사 등 여러 산업군 고객에게 공급하면서 시장에서 영향력을 강화하고 있다.

김광수 사이버아크코리아 부장은 "사이버아크는 사용자 뿐만 아니라 비 사용자와 디바이스까지 모든 대상으로 하는 일관된 접근제어 솔루션을 제공하고 있다. 사이버아크 통합 인증 플랫폼은 인가된 사용자, 애플리케이션, 디바이스에 대한 접근 방법, 시간, 대상 시스템 등을 통제하며, 모든 접근과 작업 내용을 철저히 기록한다. 이를 통해 일반 사용자, 클라우드 관리자, 네트워크 관리자, 시스템 관리자, 개발자, 보안 관리자, 감사 등 모든 사용자에게 통합된 접근과 보안 솔루션을 제공한다"고 말했다.

굿모닝아이텍이 공급하는 시큐어키의 '시큐어키 PAM'도 국내외 여러 산업군 고객으로부터 호평을 받으면서 시장 점유율을 높이고 있다. 시큐어키 PAM은 생체인증, 접근통제, 비밀번호 관리 시스템과 PAM에 필요한 기타 여러 기능을 통합했으며, 멀티·하이브리드 클라우드를 지원한다.

적시(JIT) PAM을 위한 제로 스탠딩 권한(ZSP) 정책을 적용해 지속적이고 상시적인 특권 액세스를 제거하며, 액세스와 권한 사용이 필요한 경우에만 자동으로 부여한다. 이를 통해 특권권한을 탈취한 공격자 혹은 특권 권한 사용자가 실수·고의로 대규모 사고를 일으키지 못하게 한다.

시큐어키는 온프레미스, 클라우드 환경에서 모든 유형의 아이덴티티를 보호하는 통합 솔루션을 제공한다. 어플라이언스, 가상 어플라이언스, 클라우드 SaaS로 제공되며, 온프레미스와 멀티·하이브리드 클라우드 환경에서 중단없는 제로 트러스트 아이덴티티 요구가 지켜질 수 있게 한다.