해킹 속도에 대한 액세스 관리 가속화

Chris Sullivan은 Courion에서 고급 솔루션 담당 부사장입니다. 신 제품과 솔루션을 개발해서 시장에 출시하는 한편, 업계의 현행 문제점을 효과적으로 해결하는 최신 아이디어를 배양하고 혁신하는 일을 담당하고 있습니다. Chris는 이전에 구주 및 중동거점 운영, 고급 솔루션, 고객 솔루션 및 전문 서비스 담당 부사장을 역임했습니다. 또한, Chris는 ISACA의 액세스 위험 벤치마킹 위원회(Access Risk Benchmarking Committee)의 회장이며 European Identity Conference, Gartner Catalyst Conference, MIT International Science and Technology Initiatives(MISTI), IT GRC 포럼 및 ISACA ISRM 컨퍼런스 등을 비롯한 산업 컨퍼런스에서 연사로 활발하게 활동하고 있습니다.

조직은 매일 거의 매 분마다 네트워크 액세스를 허용합니다. 해커는 내부자 액세스 자격증명을 사용해서 네트워크에 침입하려고 시도하는 경우가 많습니다. 그러나 대부분의 IT 부서는 아직도 분기별 또는 6개월마다 액세스 권한을 검토하는데 그치고 있습니다.

심지어 매월 액세스 권한을 검토하는 (오늘날의 표준에 따라 부지런한 경우) 조직조차도 하루 24시간 활동하고 있는 해커를 따라잡기에는 역부족입니다. 시스템에서 침입자를 막기 위해 매일 분투하는 네트워크 보안 직원은 자신들이 지속적으로 포위당하고 있다는 사실을 간과하기 쉽습니다. 심지어 월 단위로 액세스를 인증하더라도 침입자나 악의적인 내부자가 몰래 들어와서 피해를 입히고 다음 인증이 도래하기 전에 자신의 종적을 감추기에 충분한 무방비 기간이 있게 됩니다.

8000만 고객 및 직원 정보가 있는 Anthem 데이터베이스를 침투한 공격은 유명한 사례입니다. 2014년 5월에 침투가 발생했지만 2015년 초까지 이를 발견하지 못했습니다. 대부분은 아니지만 많은 데이터 유출에 있어서 이와 같은 늑장 대응이 발생하고 있습니다. Verizon 2015 *Data Breach Investigations Report*(DBIR)에 따르면 60퍼센트의 해킹이 단 수분이나 수초 만에 발생했습니다.[1] 61개 국가의 70개 글로벌 조직을 설문 조사한 보고서에 따르면 조사에서 테스트된 사용자 중 무려 50퍼센트 정도가 이메일을 열어서 처음 1시간 내에 피싱 링크를 클릭했습니다.

비교해 보면 사건의 75퍼센트가 수 주의 시간 후에 감지되었는데, 이러한 사건 모두가 회사의 실수로 인해 발생한 것은 아니었습니다. 보고서는 "우리는 정보 공유의 속도와 공격 속도 사이의 격차를 해소할 필요가 있다"라고 결론을 내립니다.

유사한 보고서에서는 공격 대상 네트워크 상에서 해커의 활동이 발견되기까지 평균 229일이 걸린다고 밝히고 있습니다.[2] 이러한 현실에서 IAM(Identity and Access Management)에 대한 새로운 방법이 절실하게 요구됩니다.

세분화된 보안

개방형 접근에 대한 요구는 오늘날 액세스 인증 프로세스를 압도하는 빅 데이터 크러쉬에 기름을 붓고 있습니다. 비즈니스 세계에서 소비자 액세스 모델은 쉽게 변하지 않습니다. 직원, 계약자 및 벤더 등은 웹 사이트, 직접 로그인 및 모바일 응용 프로그램 등과 같은 모든 온라인 및 모바일 채널을 통해 액세스하기를 기대합니다. 모든 새로운 액세스 포인트가 등장하게 되는 경우는 해커에게 있어서 회사의 핵심자산에 침투하는데 있어 가장 선호하는 도구인 합법적 네트워크 액세스 자격증명이라는 또 다른 기회를 제공합니다.

데이터 절도범은 피싱, 멀웨어 첨부, 그리고 도난 또는 훼손된 자격증명 등과 같이 수 년간 사용되고 있는 것과 동일한 전술을 사용해서 네트워크에 잠입하고 있습니다. 새로운 액세스 옵션은 이러한 전술을 더욱 쉽고 효과적으로 사용할 수 있도록 만들었습니다.

예를 들어, 이메일 피싱은 합법적 이메일 주소가 더 많은 곳에 게시되어 있기 때문에 이제는 더 쉬워졌습니다. 모바일 앱은 일반적인 보안 베팅을 거치지 않을 수 있지만, 직접적인 네트워크 액세스를 제공합니다. 해커가 일단 합법적 로그인 ID 또는 이메일 주소를 사용해서 내부로 침입하면, 핵심적인 시스템에 대한 액세스를 요청할 수 있게 됩니다. 또는, 멀웨어나 허위 웹사이트를 사용해서 관리자 자격증명을 도용하고, 자신에게 액세스 권한을 부여한 다음, 자신이 원하는 것을 손에 넣은 후에 종적을 감출 수 있습니다.

너무도 많은 문이 네트워크로 열려 있는 상황에서, 대부분의 조직은 내부로부터 거의 지속적인 공격을 받고 있습니다. 침입자 또는 악의적인 내부자에 대해 효과적으로 방어하려면 미사용 계정을 제거하고, 비정상적인 활동을 정확히 파악하고, 직원의 역할에 부합하지 않는 권한을 파악해야 합니다. 이렇게 하려면 네트워크 관리에 있어서 새로운 마이크로 인증 모델이 필요합니다.

마이크로 인증은 의심스러운 활동 및 이벤트로 인해 트리거되는 경우에 액세스 권한을 사업 정책에 대해 지속적으로 검증합니다. 위반 사항이 발견되는 경우, 관련 관리자에게 즉시 통보해서 교정 조치를 취하도록 합니다. 관리자는 비정상적인 경우에 대해서만 대응하며 규정을 준수하는 사용자 계정을 지속적으로 재인증하지 않습니다.

마이크로 인증의 문제점은 오늘날 대부분의 회사가 마이크로 인증을 지원하기 위해 필요한 전사적 IT 보안 프레임워크 또는 기술 도구를 보유하고 있지 않다는 사실입니다. 오늘날 IT 환경에서 일반적으로 사용되는 솔루션은 규정 준수 검토를 자동으로 실행하지만 정기적 또는 기간제 감사 확인만 제공합니다. 이러한 방법은 90일부터 심지어 30일까지의 검토 주기 사이에 대규모 무방비 상태를 만들게 됩니다. 액세스 권한을 더욱 자주 검토하는 방법은 오늘날 널리 사용되는 수동 프로세스로 인해 엄두도 못낼 정도로 비용이 많이 들며 실질적으로 거의 불가능합니다. 관리자가 수 일마다 모든 보고서를 인증하는 일은 너무나도 많은 시간이 소요되기 때문에 다른 업무를 거의 진행할 수 없게 됩니다. 사업 생산성이 심각하게 감소됩니다.

신원 및 액세스 관리에 최적화된 임베디드 데이터 분석 형태의 인텔리전스는 사인오프가 필요한 비정상적인 사용자만 보고함으로써 관리자가 수행해야 할 인증 수를 줄일 수 있습니다. 지능형 시스템에서, 관리자는 고위험 조합이 존재하거나 권한이 직원의 역할을 벗어나는지 여부를 확인하기 위해 액세스 권한을 비교 및 대조할 필요가 없습니다. 시스템은 위험을 파악해서 예외를 얼마나 수용하는 경우에 직원의 위험 등급이 높아질 것인지 계산합니다. 매니저에게는 예외가 필요한지 여부와 위험이 정당한지 여부에 대한 결정만 남습니다.

> "보안은 전략적인 우선 사항이며, COBIT는 조직이 보안을 최전선 활동으로 변환할 수 있도록 해줍니다."

COBIT를 통한 결합

마이크로 인증을 구현하려면 통합 IT 보안 아키텍처와 빅 데이터 분석 도구라는 2가지 요소가 필요합니다. ISACA가 개발한 COBIT® 5 거버넌스 맵은 대부분의 신원 및 액세스 관리 시스템의 현행 조각 이어붙이기 특성에서 발생되는 문제를 해결합니다.

COBIT®는 사업적 고려 사항(예를 들어, IT를 사업적 목표에 전략적으로 부합) 이외에도 위험, 자원 및 성과 관리를 포함하는 정합적 프레임워크에 보안을 통합합니다. IT 위반에 의해 야기되는 위험이 너무 심각한 경우, 전략적 목표와 IT 사이에 이러한 연결을 생성하는 것은 필수적입니다. 보안은 전략적인 우선 사항이며, COBIT는 조직이 보안을 최전선 활동으로 변환할 수 있도록 해줍니다.

COBIT는 전략적 목표 실행에 필수적인 목표 및 목적을 정의하기 위한 공통 언어를 제공합니다. 또한, IT 보안을 위한 목적 및 측정 기준을 정의합니다. 측정 기준은 침입자를 노출시킬 수 있는 행동 패턴을 파악하기 위해 액세스 관리 기능을 정합적 프로세스로 결합하기 위한 매개변수 역할을 합니다.

기사가 흥미롭습니까?

- 지식 센터에서 액세스 제어 및 빅 데이터에 대해 자세히 알아보고, 논의하고, 협력하십시오.

www.isaca.org/knowledgecenter

COBIT는 대부분의 IAM에 존재하는 단편화 문제를 해결합니다. 액세스 관리 벤더는 작업을 자동화하기 위한 광범위한 도구를 개발했습니다. 그러나, 침입자를 탐지하기 위한 인텔리전스를 생성하는 작업은 여전히 기본 데이터 인텔리전스가 없는 관리 도구와 수동 프로세스의 몫으로 남겨져 있습니다.

Gartner 분석가인 Brian Iverson은 "효과성 측정 기준에 공급하기 위한 데이터를 생성하는 일은 쉽지 않다"라며 "IAM 공간에 있는 대부분의 제품은 사용자 액세스에 대한 통제를 입증하기 위해 필요한 기본 프로세스 요소를 충분하게 파악하고 있지 못하고 있다. 또한, 이러한 제품은 분석, 보고 및 대시보드를 지원하는 성능 면에서도 변동 폭이 심하다. 제품의 내장 대시보드를 사용하고 싶은 경우라도, 일부 원하는 측정 기준을 얻기 위해서는 데이터를 외부에서 처리해야 할 수 있다"고 언급했습니다.[4]

자동화 격차

대부분의 기업 IT 환경에서는 자동화된 지능형 데이터 분석 도구가 부족하기 때문에 기업은 수동 액세스 관리를 사용해서 작업해야 합니다. IT 팀은 자신의 직속 부하에게 허용한 권한 목록이 있는 보고서를 각 비즈니스 관리자에게 제출합니다. 관리자는 권한이 적절한지 또는 수정되어야 하는지 여부를 입증하게 됩니다. 시스템 관리자도 동일한 일을 합니다. 이렇게 되면 세부적인 단계로 넘어감에 따라 기하 급수적으로 증가하는 엄청난 양의 데이터 세트를 수동으로 분석하게 됩니다

일반적으로, IT 직원은 데이터베이스와 애플리케이션에서 사용자 데이터를 추출해서 일반 플랫 파일로 저장합니다. 주로 보안 팀에 해당되는 다른 IT 직원 그룹은 이러한 무질서한 데이터를 스프레드시트 응용 프로그램에서 분류될 수 있는 형식으로 조정해야 합니다. 이러한 프로세스에 필요한 난이도와 비용은 중요 시스템에 대한 부적절한 액세스를 위해 자격증명이 사용될 수 있는 위험성을 더욱 높여주는 주요 요소가 됩니다. 이것은 연간 몇 회 이상 진행하기에는 너무 힘든 작업입니다. 침입자를 보여주는 비정상적인 사용 패턴을 탐지하려는 조직에 있어서는 문제점이 훨씬 심각하게 나타납니다.

10명의 직속 부하를 가진 관리자를 예로 들겠습니다. 각 직속 부하는 최소한 10개 시스템에 대한 액세스 권한을 가집니다. 각 직원은 이러한 10개 시스템 내에서 수십개의 자격을 가질 수 있습니다. 팀은 각 관리자에 대해 이렇게 많은 데이터를 분석해야 하고, 관리자는 각 데이터 포인트를 입증해야 합니다. 일부 관리자는 구체적인 세부 사항을 요구할 수 있습니다.

이러한 시나리오를 회사 수준으로 옮겨 본다면 데이터 수량이 얼마나 기하 급수적으로 증가해서 수동 분석으로 이를 감당할 수 어렵게 되는지 알 수 있습니다. 회사에 10,000명의 직원이 있고, 각 직원이 10개의 응용 프로그램을 액세스할 수 있다면 100,000개의 계정이 있는 것입니다. 보수적인 관점에서 사용자가 하루에 2회 로그인한다고 가정하겠습니다. 이런 경우 하루에 200,000회의 로그인 활동이 발생합니다. 1개월이면 4백만개의 로그인 활동 레코드가 발생합니다.

부적절한 사용을 탐지하기 위해 회사는 각 응용 프로그램 내에서 직원이 어떤 활동을 했는지도 알아야 합니다. 이와 동일한 10,000명의 직원이 하루에 50개 데이터 자산을 액세스한다고 가정하는 경우, 하루에 500,000개의 활동 레코드가 발생하고 매월 1000만개의 레코드가 발생합니다. 로그인 레코드의 경우, 매월 1400만 데이터 요소를 분석해야 합니다.

이렇게 큰 데이터 세트 전체를 수동으로 분석하는 것은 불가능합니다. 자동화를 사용하지 않는 경우 IT 조직은 특정 위험 영역만 감시하게 되어 보안 구조에 침입자가 악용할 수 있는 많은 격차가 발생합니다.

빅 데이터 방식

빅 데이터 관리 및 자동화 분석 도구가 개발되면서 의심스러운 활동을 탐지할 수천만 데이터 포인트를 지속적으로 분석함으로써 이러한 격차를 줄일 수 있게 되었습니다. 영업, 마케팅 및 고객 서비스 등과 같은 분야에서는 거의 동일한 도구가 널리 사용되었음에도 불구하고 불과 2년 전까지만 해도 IT에는 이러한 도구가 없었습니다. 빅 데이터 분석 도구는 IT에서 지속적으로 기반을 다져가고 있습니다.

미국 메사추세츠에 있는 의료 서비스 업체인 Harvard Pilgrim은 IAM에 신원 분석 및 인텔리전스를 조기 도입한 기업 중 하나입니다. 120만명 이상의 가입자를 확보하고 있는 이 회사는 매월 수천만 레코드를 관리하고 있습니다. 회사는 모든 중요 위험 분야를 모니터링하기 위한 솔루션을 구현했습니다. IT 직원은 그 어떠한 중요 분야 중에서도 미사용 계정을 삭제하는 일과 시스템을 변경하고 유지 보수를 수행할 수 있는 특권 계정을 면밀하게 관찰하는 일을 집중적으로 진행했습니다.

Harvard Pilgrim의 지능형 IAM 솔루션은 지정된 시간동안 액세스하지 않은 계정을 보고함으로써 해커가 미사용 계정을 악용하기 전에 이것을 비활성화할 수 있는 기능을 관리자에게 제공합니다. 또한, 특권 계정을 정기적으로 분석해서 현재 가지고 있는 액세스 권한과 가져야 하는 액세스 권한을 비교 확인합니다. 분석은 자동으로 지속적으로 실행되며 관리자에 의해 결정되고 액세스 관리 솔루션에 명시되어 있는 표준을 벗어나는 활동을 감지합니다. Harvard Pilgrim은 이러한 인텔리전스를 특권 액세스 계정의 수를 줄이고 불필요한 액세스 권한을 가진 계정을 제거하기 위해 사용했습니다.

또 다른 예로, 미국 플로리다주 마이애미에 있는 Children's Hospital은 동일한 방식을 구현해서 액세스 환경을 지속적으로 스캔했습니다. 자동 스캔으로 수백만개의 데이터 포인트를 분석한 결과 수백개의 미사용 계정과 회원이 없는 여러 사용자 그룹을 발견했습니다. 이렇게 발견된 각 항목은 피해가 발생된 이후까지 감지되기 어려운(불가능하지 않은 경우) 데이터 절도 위험을 보였습니다.

두 가지 경우 모두에서, IAM 방법에 신원 분석이 추가됨에 따라 IT와 비즈니스 관리자는 다음과 같은 질문에 응답함으로써 고위험 개인 및 그룹을 즉각적으로 파악할 수 있었습니다.

- 암호가 변경된 도메인 관리자 계정이 있는가?
- 영업 직원이 액세스한 비영업 시스템은 무엇인가?
- 반드시 알아야 필요가 없이 환자 의료 정보를 액세스한 사람이 있는가?
- 최소한 5개의 권한을 가진 계정으로서 30일이 넘도록 사용되지 않은 것은?
- 이 계정에 의심스러운 수의 특별 권한이 있는가?
- 파트타임 직원이 일반적으로 허용되는 모든 액세스 권한을 받아야 하는가?
- 프로젝트가 종료된 후에 계약자가 자원을 계속해서 액세스하는가?
- 시스템 관리자에게 일반적으로 업무 수행에 필요 없는 권한이 지정되는가?
- 이 사업부가 불필요한 권한이 있는 비정상적인 수의 계정을 가지고 있는가?

회사가 이러한 방식을 취하지 못하도록 방해하는 기술적인 제한 사항은 없습니다. 소비자 영역에서, Amazon.com은 쇼핑 습관을 추적하기 위해 수 년간 매우 유사한 일을 해오고 있습니다. 이를 통해 고객이 조회하는 제품과 조회 시기를 파악해서 회사가 홍보 행사와 구매 인센티브를 제공할 수 있도록 하는 것입니다. 신용 카드 회사에서도 동일한 방법이 진행됩니다. 의심스러운 구매가 발생하는 경우에 이를 거의 즉각적으로 감지하고, 고객에게 알리고, 감지한 후 수 분 내에 카드를 취소해서 손실을 예방합니다.

마찬가지로, 시장에서도 어플리케이션 프로그래밍 인터페이스(API) 또는 스크립팅을 통해 작업함으로써 수동 데이터 추출이 필요 없도록 해주는 IAM 솔루션이 있습니다. 이것은 분석을 위해 데이터를 자동으로 청소하고 분석 인텔리전스를 자동으로 적용해서 네트워크 상에 작업을 진행하고 있는 사람과 시점을 확인하기 위한 필수적인 질문에 응답합니다.

지능형 액세스 관리 지향적

오늘날 비즈니스의 진행 속도는 IT 자원에 대한 오픈 액세스의 증가를 요구하고 있습니다. 이러한 액세스에서는 합법적인 액세스 포인트, 자격증명 및 사용자 계정을 사용해서 민감한 데이터 자원을 공격하는 침입자를 통해 데이터 절도 또는 손상의 위험이 더욱 커집니다.

오늘날 대부분의 기업 IT 환경을 차지하고 있는 액세스 관리 솔루션에 있어서, 위험을 개선하기 위해 이러한 자원의 부적절한 사용을 파악하기 위하여 액세스 권한을 지속적으로 모니터링하는 것은 거의 불가능합니다. 중요 응용 프로그램 및 데이터베이스로 통합된 기본 액세스 관리 및 보안 도구를 중심으로 구축된 IT 보안 인프라는 세분화됩니다. 이러한 세분화는 보안 데이터를 분석하고 액세스 권한을 인증하는 수동 프로세스에 대한 의존도에 기여합니다. 이러한 방식은 느리고 비용도 많이 들며, 오늘날 소비자로부터 영감을 받은 오픈 액세스 환경에 의해 생성된 엄청난 양의 데이터를 수용할 정도로 확장될 수 없습니다.

그러나, 동일한 소비자 모델도 문제점에 대한 해답을 포함하고 있습니다. 소비자 어플리케이션에 사용되는 것과 맞먹는 빅 데이터 분석 도구는 액세스 데이터를 지속적으로, 신속하게, 경제적으로 분석할 수 있는 능력을 제공함으로써 마이크로 인증 액세스 관리 모델을 지원합니다. 마이크로 인증 시스템은 비정상적인 활동을 파악해서 잠재적인 위험 상황이 발생하는 경우에만 비즈니스 관리자가 대응하도록 요구합니다. 관리자가 과도하고, 중복적이고, 불필요한 인증으로 교착 상태에 빠지지 않도록 하면서 지속적인 딜리전스를 허용합니다.

IT 조직은 해커보다 한 발 앞서 나가려면 자동화 및 인텔리전스 전략을 도입해야 합니다. 이렇게 하지 않는 경우, 더욱 광범위한 액세스에 대한 요구가 증가하고 네트워크로 더 많은 문이 열림에 따라, 데이터 해커가 수 분 안에 공격하고, 수 초만에 사라지고 수 년간의 손해를 유발하는 동안 기업은 계속해서 몇 주가 지난 후에야 대응 시간을 측정하게 됩니다.

“IT 조직은 해커보다 한 발 앞서 나가려면 자동화 및 인텔리전스 전략을 도입해야 합니다.”

미주

[1] Verizon, 2015 *Data Breach Investigation Report, www.verizonenterprise.com/DBIR/2015/*

[2] Mandiant, *M-Trends 2014: Beyond the Breach, http://connect.mandiant.com/m-trends_2014*

[3] Frisken, John; “Leveraging COBIT to Implement Information Security,” *COBIT Focus*, ISACA®, USA, 4 May 2015, *www.isaca.org/cobitfocus,* figure 2.

[4] Iverson, B.; *Demonstrate Control Over User Access With IAM Effectiveness Metrics*, Gartner, 5 February 2015, *www.gartner.com/doc/2978217/demonstrate-control-user-access-iam*