백서 • 2017년 5월

결제 카드 산업 데이터 보안 표준과 CA Privileged Access Management

목차

소개

PCI DSS(Payment Card Industry Data Security Standard)는 신용 카드 소지자 데이터에 대한 관리를 강화하고 신용 카드 사기 위험을 줄이기 위해 2004년 처음으로 도입되었습니다. 매년 검증을 실시해야 하고, 주기적으로 새로운 개정판을 내놓으면서 표준도 계속 발전해 왔습니다. 최신판은 버전 3.2로 2016년 4월에 발효되었습니다. 2018년 1월 말까지 PCI DSS와 PA-DSS(Payment Application Data Security Standard)는 구현 베스트 프랙티스로 간주되고 2018년 2월 1일부터는 요구 사항으로 간주됩니다.

섹션 1

PCI DSS 3.2의 주요 요구 사항

PCI DSS의 주요 요구 사항은 다음과 같습니다.

PCI 데이터 보안 표준 - 개요

보안 네트워크 및 시스템 구축, 유지 관리	1. 카드 소지자 데이터를 보호하는 방화벽 구성을 설치하고 유지 관리 2. 공급업체에서 제공하는 기본값을 시스템 암호 및 기타 보안 매개 변수로 사용하지 말 것
카드 소지자 데이터 보호	3. 저장된 카드 소지자 데이터 보호 4. 개방된 퍼블릭 네트워크를 통해 전송되는 카드 소지자 데이터 암호화
취약성 관리 프로그램 유지	5. 맬웨어로부터 모든 시스템을 보호하고 바이러스 백신 소프트웨어 또는 프로그램을 정기적으로 업데이트 6. 보안 시스템 및 애플리케이션 개발 및 유지 관리
강력한 액세스 제어 수단 구현	7. 업무상 알아야 하는 경우에만 카드 소지자 데이터에 대한 액세스 허용 8. 시스템 구성 요소에 대한 액세스를 식별하고 인증 9. 카드 소지자 데이터에 대한 물리적 액세스 제한
정기적으로 네트워크 모니터링 및 테스트	10. 네트워크 리소스 및 카드 소지자 데이터에 대한 모든 액세스 추적 및 모니터링 11. 보안 시스템 및 프로세스 정기 테스트
정보 보안 정책 유지 관리	12. 모든 직원에 대한 정보 보안을 다루는 정책 유지 관리

전체적으로 광범위한 보안 조치를 다루는 요구 사항입니다. 그러나 이 문서에서는 권한 있는 사용자(privileged user) 관리에 관련된 요구 사항을 살펴봅니다.

권한 있는 액세스 관리가 중요한 이유

흔히 말하듯이 체인에서 가장 약한 고리의 강도에 따라 체인의 견고함이 결정됩니다. 가장 약한 고리는 잘 보이지 않는 경우가 많습니다. 권한 있는 ID는 규정 준수 위반이나 실패의 형태로 불편한 진실이 드러나기 전까지 거의 노출되지 않습니다. 권한 있는 액세스의 몇 가지 주요 측면은 다음과 같습니다.

어디에든 존재. 어느 조직에나 특정 애플리케이션에 대해 높은 액세스 권한을 가진 사용자가 있습니다. 가장 눈에 띄는 사용자는 관리 권한을 가진 사용자입니다. 그러나 소프트웨어 개발의 변화와 디지털 혁신에 따라 권한 있는 액세스를 보유한 ID의 성격이 크게 바뀌고 있습니다. 조직이 인프라, 플랫폼, 애플리케이션을 위한 가상 환경 및 클라우드로 이동하면서 부서 내의 사용자는 추가적인 권한을 얻었습니다. 애자일 방법론의 채택은 A2A(Application-to-Application) 상호 작용을 증가시켰습니다. 이런 변화는 빙산의 일각일 뿐이며 앞으로 더 많은 변화가 일어날 것입니다.

큰 영향력. 애플리케이션이나 인프라에 대한 권한 있는 액세스에는 중대한 책임이 따른다는 것은 분명합니다. 그러한 사용자나 ID는 민감한 데이터에 액세스할 수 있으며, 악의적인 액세스나 우연한 사고로 인해 중대한 피해를 주고 회사의 명성을 위협할 수 있습니다. 앞서 언급한 각각의 예에서 사용자가 우연히 또는 일부러 미션 크리티컬 서버의 데이터를 삭제하거나 감독을 받지 않고 운영 서버의 구성을 변경한다면 실제 비즈니스에 영향을 미치고 우려를 일으킬 수 있습니다.

선호되는 표적. 권한 있는 사용자와 ID의 액세스가 얼마나 중요한지 생각하면 해를 입히려는 사람이 이들을 노릴 가능성이 큽니다. 이들은 공격의 표적이 되는 경우가 매우 많으며 조직이 적절한 보안 태세를 유지하지 않으면 공격에 영향받을 가능성이 매우 큽니다.

위와 같은 이유로 권한 있는 사용자 액세스 관리는 매우 중요합니다. 또한 업종에 따라 직접적으로든 간접적으로 규정에 의해 그러한 액세스를 부여해야 할 수 있습니다. PCI DSS는 그러한 의무 규정을 두고 있습니다. 실제로 버전 3.2에 도입된 변경 사항은 권한 있는 액세스의 관리 방식에 직간접적으로 많은 영향을 미칩니다. 이 문서의 나머지 부분에서는 권한 있는 액세스에 적용되는 PCI DSS 3.2의 구체적인 요구 사항을 검토합니다.

권한 있는 액세스 관리와 PCI DSS 3.2

버전 3.2에서는 PCI DSS 표준의 몇몇 섹션을 개선하여 변화하는 비즈니스 현실을 반영했습니다. 이러한 변경 사항 일부가 권한 있는 액세스의 관리 방식에 적용됩니다. 다음 표에서는 PCI DSS에 정의된 요구 사항 및 이러한 요구 사항과 권한 있는 액세스 관리의 관련성을 자세히 설명합니다.

요구 사항	버전 3.2의 변경 사항	권한 있는 액세스 관리에 미치는 영향
요구 사항 1: 카드 소지자 데이터를 보호하는 방화벽 구성을 설치하고 유지 관리	이 요구 사항을 반영하도록 여러 섹션을 변경하고, 1.3.3은 삭제되었습니다.	이 요구 사항은 방화벽 구성에 대한 액세스 권한이 있는 사용자 그룹 및 역할을 관리할 필요성을 규정합니다. 또한 권한 있는 액세스 관리가 다음 조건을 충족할 것을 암묵적으로 요구합니다. • 카드 소지자 데이터 환경에서 나가는 아웃바운드 트래픽이 없도록 보장 • 구성 파일의 모든 변경 사항을 관리하고 모니터링
요구 사항 2: 공급업체에서 제공하는 기본값을 시스템 암호 및 기타 보안 매개 변수로 사용하지 말 것	이 버전에서는 대체로 부연 설명만 추가되었습니다.	이 섹션은 권한 있는 ID 및 액세스에 광범위한 영향을 미칩니다. 오늘날 대부분의 소프트웨어와 하드웨어는 기본 암호가 설정되어 배송됩니다. 또한 이러한 암호에 대한 정책은 상당히 제각각입니다. 우선은 표준의 요구 사항 범위에 포함되는 모든 자산을 식별해야 합니다. 이러한 자산은 온프레미스, 가상 또는 여러 클라우드 환경에 존재할 수 있습니다. 권한 있는 액세스 관리 솔루션은 이러한 자산을 발견하도록 지원할 뿐만 아니라 암호에 대한 정책 설정을 지원하고 세션을 기록하고 모든 영역(클라우드, 가상, 온프레미스)에서 이러한 자산에 대한 액세스 제어를 지원합니다. 마지막으로, 액세스 제어는 이러한 시스템의 모든 보안 구성 변경 사항을 안전하게 보호하고 모니터링하기에 충분할 정도로 세밀해야 합니다.

요구 사항 5: 맬웨어로부터 모든 시스템을 보호하고 바이러스 백신 소프트웨어 또는 프로그램을 정기적으로 업데이트	변경 사항 없음	맬웨어 방지 방법은 다양합니다. 요구 사항에는 바이러스 백신 소프트웨어가 베스트 프랙티스로 명시되어 있지만 조직에서는 맬웨어를 방지하는 모든 수단을 고려해야 합니다. 권한 있는 액세스 관리를 통해 조직에서 맬웨어를 방지할 수 있습니다. 예를 들면 바이러스 백신 프로그램이 설치된 시스템의 경우 업그레이드 및 유지 관리를 위한 관리 액세스를 적절히 제어해야 합니다. 카드 소지자 데이터가 보관되는 다른 시스템의 경우 격리 전략을 구현하고 애플리케이션과 인프라를 분류하며 해당 시스템에 대한 액세스를 제어할 수 있습니다. 또한 사용자가 실행하는 명령을 제한할 수 있습니다. 나아가 머신러닝과 사용자 행동 분석의 발전을 통해, 계정이 탈취된 경우에도 의심스러운 활동을 사전에 제지할 수 있습니다. 이는 조직이 직면하는 당면 과제의 규모와 범위를 고려하여 수동적 방법이 적절하지 않을 때 훨씬 더 중요합니다. 마지막으로 권한 있는 액세스 관리 솔루션은 키로깅, 화면 녹화와 같은 기술을 사용하여 활동을 모니터링하고 기록할 수도 있게 해줍니다.
요구 사항 6: 보안 시스템 및 애플리케이션 개발과 유지 관리	특정 섹션에 한정되어 변경되었으며 지침용입니다.	이 섹션에서는 카드 소지자 데이터에 액세스하는 소프트웨어 및 시스템을 개발하고 유지 관리할 때 따라야 하는 전체적인 보안 베스트 프랙티스를 다룹니다. 이 요구 사항의 지침에는 다음과 같은 측면이 포함됩니다. • 가장 최신 패치가 시스템에 적용되도록 보장 • 올바른 보안 절차를 따르는 소프트웨어를 개발 • 운영 및 비운영 애플리케이션, 서버를 분리 권한 있는 액세스 관리 솔루션은 이 요구 사항을 해결하는 데 크게 도움이 될 수 있습니다. 예를 들어 시스템을 유지 관리하고 패치 등을 적용할 때 조직은 적절한 수준의 인증 및 감독을 받는 충분한 제어 절차를 마련해야 합니다. 예를 들면 관리자 권한을 가진 사용자가 명령을 실행하여 서버를 패치하는 것이 허용되지만 운영 시스템인 경우에는 추가적인 제어와 승인을 적용해야 할 수 있습니다. 애플리케이션은 프로그램적 방법으로 카드 소지자 데이터에 액세스할 수 있지만 이렇게 하려면 자격 증명이 필요합니다. 마지막으로 이 요구 사항은 다양한 환경에 액세스하는 사용자의 직무(개발자, 테스트, 운영 환경) 분리에 대한 필요성을 다룹니다. 권한 있는 액세스 관리 솔루션은 이러한 자격 증명을 애플리케이션 내에 포함하지 않고 관리하는 데 도움이 될 수 있습니다. 직무 분리 요구 사항은 권한 있는 액세스 관리 솔루션과 자동화 도구를 통합하여 충족할 수 있습니다.

요구 사항 7: 업무상 알아야 하는 경우에만 카드 소지자 데이터에 대한 액세스 허용	멀티 시스템을 포괄하기 위해 지침과 테스트가 변경되었습니다.	이 요구 사항은 민감한 데이터가 포함된 애플리케이션이나 시스템에 대한 다양한 사용자의 액세스를 역할, 업무상 필요, 최소 권한을 기반으로 제어해야 할 필요성에 대해 다룹니다. 그러한 액세스는 로깅되고 감사할 수 있어야 합니다. 권한 있는 액세스 관리 솔루션은 사용자를 그룹으로 관리하고 특정 애플리케이션이나 애플리케이션 그룹의 사용자에게 허용되는 작업을 정의함으로써 이 요구 사항을 해결하도록 지원합니다. 또한 다른 솔루션과의 통합을 활용하여 다양한 애플리케이션과 시스템에 대한 워크플로우 기반의 액세스 프로비저닝 및 디프로비저닝을 제공할 수 있습니다. 결국 이러한 액세스를 기록, 로깅 및 감사할 수도 있습니다.
요구 사항 8: 시스템 구성 요소에 대한 액세스를 식별하고 인증	현재 버전에서 가장 중요한 변경 사항입니다. 이제 민감한 데이터에 대한 웹 기반이 아닌 모든 원격 액세스는 MFA(Multifactor Authentication)로 보호해야 합니다. 또한 초기의 2단계 인증 요구 사항은 다단계 인증을 포함하도록 확장되었습니다.	이 요구 사항은 권한 있는 계정에 광범위한 영향을 미칠 것입니다. 직접적 또는 간접적으로든 액세스되는 모든 권한 있는 계정은 원격으로 액세스될 때 MFA로 보호해야 합니다. 모든 사용자 액세스는 로깅되고 추적 가능해야 합니다. 이 요구 사항은 그러한 시스템에 액세스하는 모든 사용자에게 고유 ID를 할당하도록 규정합니다. 사용자 액세스는 최소 권한을 기반으로 구성되고 모든 작업은 감사가 가능해야 합니다. 적절한 사용자 수명 주기 관리(프로비저닝, 디프로비저닝, 수정)가 적용되어 사용자 및 사용자 액세스를 생성, 삭제, 수정할 수 있어야 합니다. 자격 증명을 포함한 모든 사용자 정보는 강력한 암호화를 사용하여 관리해야 합니다. 모든 암호는 구체적인 강도 및 교체 정책을 준수해야 합니다. 또한 공유된 자격 증명을 특정 애플리케이션에 사용할 수 없도록 규정합니다. 카드 소지자 데이터가 포함된 데이터베이스에서는 역할과 업무상 필요(데이터베이스 관리자만 허용)를 기반으로 명령 실행을 제한하고, 그 외 모든 액세스는 거부되도록 적절하게 통제해야 합니다.
요구 사항 10: 네트워크 리소스 및 카드 소지자 데이터에 대한 모든 액세스 추적 및 모니터링	서비스 제공자 환경에서 보안 실패를 적시에 탐지하고 보고해야 하는 요구 사항이 추가되었습니다.	이 요구 사항은 네트워크의 모든 리소스에 대해 모든 사용자, 사용자 액세스 및 규칙, 구성, 특정 필드의 액세스 제어에서 발생할 수 있는 변경 사항의 완전한 감사 내역을 유지 관리해야 할 필요성을 규정합니다.

요구 사항 11: 보안 시스템 및 프로세스의 정기적 테스트	변경 사항 대부분은 권한 있는 액세스 관리에 직접적인 영향이 없는 침투 테스트 요구 사항과 관련 있습니다.	이 요구 사항의 규정 중 하나는 위험 판단을 위한 침입 탐지 시스템을 구현해야 한다는 것입니다. 그러나 컴퓨팅 환경의 변화로 인해 지금은 머신러닝 기법을 사용하여 사용자 행동을 기반으로 사전에 위협을 완화할 수 있습니다.
요구 사항 12: 모든 직원에 대한 정보 보안을 다루는 정책 유지 관리	최신 버전에서 변경된 사항 대부분은 설명과 테스트 절차에 대한 내용입니다.	권한 있는 액세스 관리 솔루션은 액세스를 제어하는 정책을 지원하고 권한 있는 사용자가 모든 직원에 대한 보안 정책을 생성, 수정, 삭제하는 것을 허용해야 합니다. 모든 작업은 감사 가능해야 하며, 해당 트랜잭션을 실행한 특정 사용자를 추적할 수 있어야 합니다.

섹션 2

CA Privileged Access Manager 및 PCI DSS 3.2의 요구 사항 지원

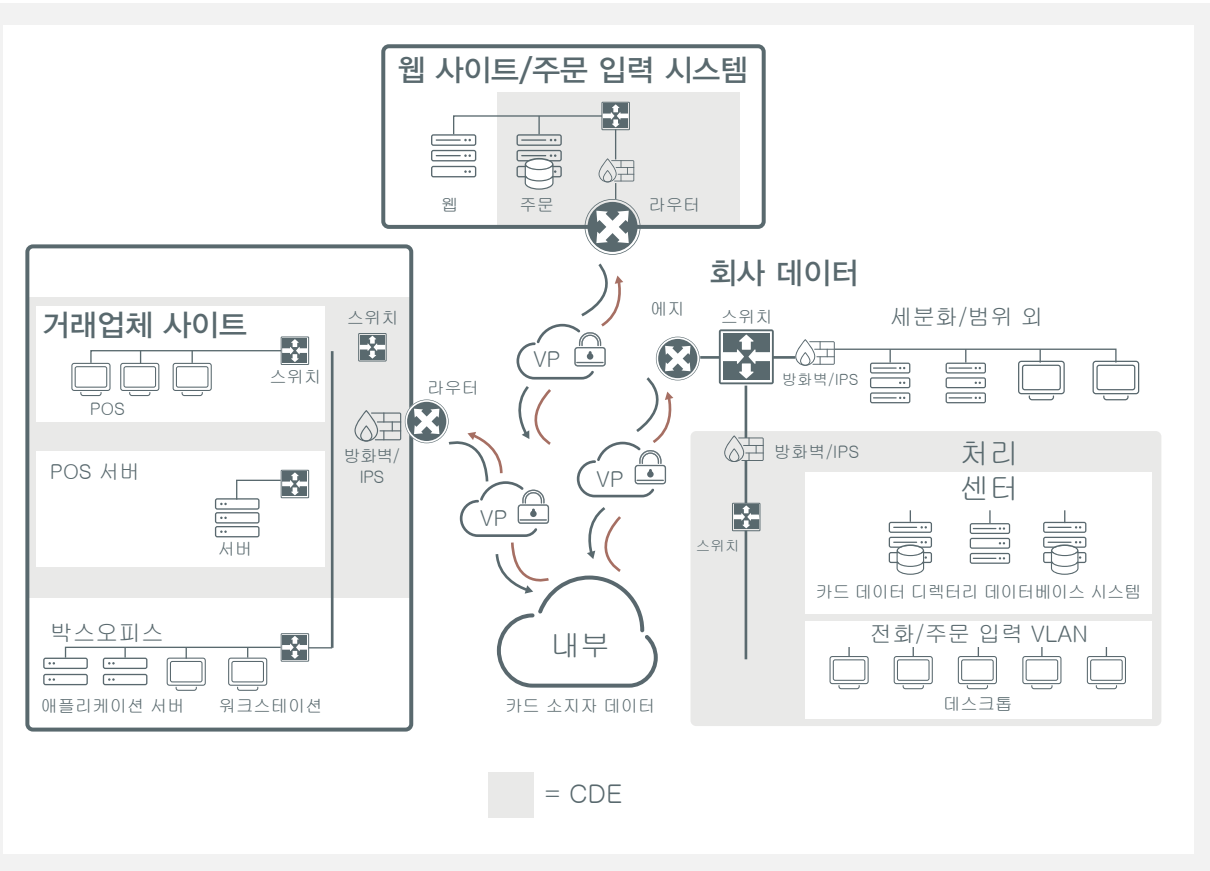
침해 킬체인 차단

킬체인의 기본 개념은 공격자가 시스템에 액세스(또는 액세스 확장)한 후 더 높은 권한을 획득하는 반복적인 패턴을 따른다는 것입니다. 이렇게 획득한 권한을 가지고 종횡무진으로 이동하여 다른 시스템에 대한 액세스를 확보하거나 기존 액세스 권한을 확장한 다음, 다시 높은 권한을 획득합니다. 최종 표적에 도달할 때까지 이런 연쇄적인 악용이 계속됩니다. 이러한 반복 과정의 어느 지점에서 연쇄적인 악용 패턴을 차단한다면 최종 표적에 도달하기 전에 공격을 중지시킬 수 있습니다.

CA PAM(CA Privileged Access Manager)은 킬체인을 차단하는 기능을 제공합니다. 예를 들어 CA PAM은 권한 있는 계정에 대한 다단계 인증을 지원합니다. 이 경우 공격자가 단일 계정에 대해 여러 자격 증명을 침해해야 하므로 권한 있는 계정을 침해하기가 어려워집니다. 또한 각 권한 있는 계정에서 각 CDE(Cardholder Data Environment) 구성 요소에 실행할 수 있는 명령과 관련해 최소 권한만 사용하면 민감한 정보에 대한 액세스를 줄이고 공격자가 관심 있는 데이터에 무단으로 액세스하는 것을 어렵게 만들 수 있습니다.

킬체인을 차단하는 또 한 가지 방법으로 CA PAM은 네트워크 세분화를 지원합니다. 즉, 특정 권한 있는 계정에서 액세스할 수 있는 서브넷과 관리할 수 있는 각 서브넷상의 시스템을 제한하는 것입니다. 네트워크 세분화를 통해 한 시스템에서 다른 시스템으로 수평 확산되는 공격을 제한하고 공격자가 조직의 네트워크를 파악할 수 없도록 제한할 수 있습니다. 비슷한 방식으로, CA PAM은 관리자가 다른 시스템에 대해 무단 네트워크 연결(예: CA PAM 정책에서 허가하지 않은 호스트로 SSH 또는 텔넷 시도)을 열지 못하게 하는 SFA(소켓 필터 에이전트)를 제공합니다.

그림 1.
PCI DSS 규정 준수를 위한 세분화



CA의 권한 있는 액세스 관리 솔루션은 조직이 PCI DSS 3.2 요구 사항을 해결하도록 지원합니다. 이 섹션에서는 솔루션의 다양한 기능을 설명합니다. 또한 다른 통합 CA 보안 솔루션과 결합하면 PCI DSS 요구를 충족하는 강력하고 확장 가능하며 완전한 기능을 갖춘 솔루션을 채택할 수 있습니다. 아래 표에서 CA PAM이 최신 PCI DSS 요구 사항 준수를 어떻게 지원할 수 있는지 자세히 설명합니다.

요구 사항	버전 3.2의 변경 사항
1.1: 방화벽과 라우터 구성 표준을 설정 및 구현한다.	CA의 권한 있는 액세스 관리 솔루션은 권한 있는 사용자의 특정 집합만 방화벽과 라우터 구성을 설정, 구현하고 관리할 수 있는 기능을 제공합니다.
1.1.5: 네트워크 구성 요소 관리에 대한 그룹, 역할, 책임을 기술한다.	CA 솔루션은 사용자 그룹을 생성하고 각 그룹의 사용자에게 구체적인 역할과 권한을 배정하여 네트워크 구성 요소, 서버, 애플리케이션 관리에 대해 직무와 적절한 책임을 구분하여 부여하는 기능을 제공합니다. 또한 VMWare NSX와 같은 가상 네트워크 환경 관리를 지원하여 포괄적이고 확장 가능한 솔루션을 제공합니다. CA 아이덴티티 관리 및 거버넌스 솔루션과 통합하면 사용자를 그룹과 역할에 배정하는 프로세스를 자동화할 수 있습니다.

1.2.1: 인바운드 및 아웃바운드 트래픽을 카드 소지자 데이터 환경에 필요한 범위로 제한하고 다른 모든 트래픽을 거부한다.	이 요구 사항은 인바운드 및 아웃바운드 트래픽에 대한 모니터링 필요성에 초점을 두고 있지만 CA Privileged Access Manager Server Control을 사용하면 서버 집합에서 특정 명령을 허용하지 않음으로써 데이터가 조직의 네트워크 밖으로 유출되지 않도록 할 수 있습니다.
2: 공급업체에서 제공하는 기본값을 시스템 암호 및 기타 보안 매개 변수로 사용하지 않는다.	CA PAM은 관리자를 위한 허용된 네트워크 액세스 방법과 같이 기본 암호의 변경 및 기타 보안 매개 변수를 지원합니다.
2.1: 공급업체에서 제공하는 기본값을 반드시 변경하고 네트워크에 시스템을 설치하기 전에 불필요한 기본 계정을 제거하거나 사용하지 않도록 설정한다.	CA PAM은 관리 암호/자격 증명을 금고(vault)에 보관하고 관리합니다. 여기에는 기본 암호의 강제 변경이 포함됩니다.
2.3: 강력한 암호화 기술을 사용하여 모든 비 콘솔 관리 액세스를 암호화한다. 웹 기반 관리와 기타 비 콘솔 관리 액세스에 SSH, VPN 또는 SSL/TLS 등의 기술을 사용한다.	CA PAM은 개인이 승인된(암호화된) 프로토콜을 통해서만 시스템에 액세스할 수 있도록 하는 액세스 정책을 시행합니다. 모든 관리 암호와 자격 증명은 암호화된 금고에 보관되기 때문에 관리자는 이러한 액세스 정책을 피할 수 없습니다. CA PAM은 관리 트래픽 도청과 조작을 방지하는 SSL VPN을 제공하며 CA PAM 콘솔에 액세스하는 것 자체가 TLS(HTTPS)로 보호됩니다.
5.1: 일반적으로 악성 소프트웨어에 영향을 받는 모든 시스템(특히 개인 컴퓨터와 서버)에 바이러스 백신 소프트웨어를 배포한다.	CA 권한 있는 액세스 관리는 특정 사용자가 시스템 집합에서 특정 애플리케이션의 설치와 업그레이드를 관리하도록 허용합니다. 이러한 허용은 관리자의 그룹이나 역할을 기준으로 할 수 있습니다. 또한 시스템과 서버를 화이트리스트나 블랙리스트에 올려 맬웨어가 확산되지 않도록 할 수 있습니다. CA Threat Analytics for PAM을 사용하면 의심스러운 활동을 탐지하고 완화 전략을 시작할 수도 있습니다.
6: 보안 시스템 및 애플리케이션 개발과 유지 관리	CA PAM을 통해 카드 소지자 데이터 처리 시스템의 일부인 스크립트, 코드 및 구성 파일에서 A2A 암호를 제거함으로써, 관리 암호가 일반 텍스트로 저장되어 애플리케이션 개발자와 테스터가 액세스할 수 있게 되는 중대한 취약점을 제거할 수 있습니다. 이 취약점은 요구 사항에서 특별히 언급되지는 않았지만, 보고 및 업스트림 또는 다운스트림 트랜잭션 목적 등으로 카드 소지자 데이터베이스에 통합된 자체 개발 시스템, 애플리케이션 및 스크립트에서 특히 리스크가 매우 높은 문제입니다.

6.3: 다음과 같이 안전하게 내부 및 외부 소프트웨어 애플리케이션(애플리케이션에 대한 웹 기반 관리 액세스 포함)을 개발한다. • PCI DSS를 따른다(예: 보안 인증 및 로깅). • 업계 표준 및/또는 베스트 프랙티스를 기반으로 한다. 소프트웨어 개발 수명 주기 전체에서 정보 보안을 통합한다.	요구 사항 6.3.1을 참조하십시오.
6.3.1: 애플리케이션을 활성화하거나 고객에게 릴리스하기 전에 개발, 테스트 및/또는 커스텀 애플리케이션 계정, 사용자 ID, 암호를 제거한다.	CA PAM을 활용하여, 조직에서는 암호를 애플리케이션 코드에서 암호화된 금고로 옮기고 CA PAM API를 사용하여 특별히 허가된 호출 애플리케이션만 암호를 요청하도록 할 수 있습니다. 네트워크와 메모리 전체에서 암호는 금고에서 대상 시스템까지 암호화된 상태를 유지합니다. 또한 CA 아이덴티티 관리 및 거버넌스 솔루션과 통합하여 애플리케이션 계정, 사용자, 자격 증명의 프로비저닝과 디프로비저닝을 관리하도록 허가된 사용자만 이 작업을 수행할 수 있습니다.
6.4: 시스템 구성 요소를 변경할 때는 항상 변경 제어 프로세스 및 절차를 따른다. 프로세스에는 다음이 포함되어야 한다.	요구 사항 6.3.1을 참조하십시오.
6.4.2: 개발/테스트와 운영 환경 간의 직무를 분리한다.	CA PAM은 개발, 테스트 및 운영에 사용되는 시스템에서 권한 있는 계정에 대해 역할 기반 액세스 제어를 시행합니다. CA PAM에 CA 아이덴티티 관리 및 거버넌스 솔루션을 통합하면 역할, 권한, 직무 분리 정책을 기반으로 적정한 수준의 사용자 액세스를 제공할 수 있습니다.
7: 업무상 알아야 하는 경우에만 카드 소지자 데이터에 대한 액세스 허용	CA PAM은 포괄적인 제어를 구현하여 시스템 구성 요소와 카드 소지자 데이터에 대한 액세스를 제한합니다. 이러한 제어를 통해 조직은 최소 권한의 개념을 "구체적인 권한이 정의되지 않으면 권한 없음"으로 확장한 제로 신뢰(zero-trust) 모델을 구현합니다. CA의 제로 신뢰 모델은 모든 권한 있는 사용자 세션에 대해 세밀한 액세스 제어, 모니터링, 기록을 시행합니다. 권한 있는 거버넌스(CA PAM과 CA 아이덴티티 관리 및 거버넌스 솔루션 통합)를 통해 모든 시스템에서 작업 생성, 판독, 업데이트, 삭제의 전체 사용자 수명 주기를 제어할 수 있습니다. 이를 통해 직무를 분리하고 규정 준수 보고를 간소화합니다.

7.1: 시스템 구성 요소 및 카드 소지자 데이터에 대한 액세스를 업무상 필요한 개인으로만 제한한다.	CA PAM은 여러 가지 방법으로 최소 권한 원칙을 구현합니다. 권한 있는 사용자에 대해 세밀한 액세스 제어를 시행하여, 서버, 네트워크 장치, 기타 시스템 구성 요소에 대한 액세스를 명시적으로 부여해야 합니다. 또한 명령 필터링(화이트리스트와 블랙리스트)을 사용하여 허가된 사용자가 실행할 수 있는 명령을 제한합니다. 권한 있는 거버넌스(CA PAM과 CA 아이덴티티 관리 및 거버넌스 솔루션)를 통해 완전한 승인 프로세스를 거쳐 사용자에게 데이터에 대한 액세스가 제공될 수 있으며, 권한 변경을 제어할 수 있고 규제를 위해 모든 액세스 권한을 보고하고 인증할 수 있습니다.
7.1.1: 다음을 포함하여 각 역할의 액세스 필요성을 정의한다. • 각 역할이 업무상 액세스할 필요가 있는 시스템 구성 요소와 데이터 리소스 • 리소스에 액세스하기 위해 필요한 권한의 수준(예: 사용자, 관리자 등)	CA PAM은 역할 기반 액세스 제어를 완전히 지원하므로 각 관리 역할(예: 데이터베이스, 네트워크 또는 시스템 관리자)의 액세스 필요성을 정의하는 데 매우 적합한 메커니즘을 제공합니다. 여기에는 각 관리 역할이 액세스할 수 있는 시스템 구성 요소와 시스템 구성 요소 내의 데이터 리소스를 제한하는 것이 포함됩니다.
7.1.2: 권한 있는 사용자 ID에 대한 액세스를 업무 수행에 필요한 최소 권한으로 제한한다.	이것은 CA PAM의 핵심 기능입니다. 각각의 권한 있는 사용자 ID 또는 권한 있는 사용자 ID 그룹은 허가된 각 시스템 구성 요소에 필요한 명령에만 액세스하도록 제한할 수 있습니다.
7.1.3: 개별 직원의 직종과 직무를 기반으로 액세스를 배정한다.	CA PAM은 개인이나 그룹에 적용되는 정책을 시행합니다. 그룹 및 역할 정의는 CA PAM에서 직접 설정하거나, 솔루션 통합을 활용하고 기업 디렉터리에 이미 있는 그룹 및 역할 정의를 사용하여 설정할 수 있습니다. 또한 CA 아이덴티티 관리 및 거버넌스 솔루션과 통합하면 비즈니스 역할, 그룹 또는 위치를 기준으로 사용자 액세스를 프로비저닝 및 디프로비저닝하는 프로세스를 더 쉽게 관리할 수 있습니다. 관리자에게 잘못 부여된 권한을 수정할 수 있습니다.
7.1.4: 필수 권한을 지정하는 권한 있는 당사자의 문서화된 승인이 필요하다.	CA PAM은 암호가 릴리스되기 전에 권한 있는 개인의 승인을 요구(및 기록)하는 이중 허가를 시행할 수 있습니다.
7.2: 시스템 구성 요소에 대해 사용자의 업무상 필요성을 기준으로 액세스를 제한하고, 명시적으로 허용하지 않는 한 "모두 거부"하도록 설정하는 액세스 제어 시스템을 구축한다. 이 액세스 제어 시스템은 다음을 포함해야 한다.	CA PAM은 인증과 허가를 분리합니다. 사용자는 강력한(다단계) 인증 방법을 사용하여 CA PAM에 로그인합니다. 그 지점부터 사용자에게는 명시적으로 액세스가 허가된 구성 요소 목록이 제공됩니다. 사용자는 허가되지 않은 구성 요소를 보거나 액세스할 수 없습니다.
7.2.1: 모든 시스템 구성 요소에 적용되어야 한다.	PCI DSS에 정의된 대로 시스템 구성 요소는 서버, 네트워크 장치, 애플리케이션을 포함합니다. CA PAM은 상용 애플리케이션을 포함하여 PCI DSS에 정의된 모든 구성 요소를 포괄합니다.

7.2.2: 직종과 직무를 기준으로 개인에게 권한을 배정한다.	CA PAM은 개인 또는 그룹 정책을 통해 개인에게 명시적으로 액세스가 부여된 경우가 아니면 모든 액세스를 거부합니다.
7.2.3: "모두 거부" 설정을 기본값으로 한다.	CA PAM은 개인 또는 그룹 정책을 통해 개인에게 명시적으로 액세스가 부여된 경우가 아니면 모든 액세스를 거부합니다.
8: 시스템 구성 요소에 대한 액세스를 식별하고 인증한다.	CA PAM은 각 사용자를 식별하기 위해 고유한 사용자 로그인을 요구하며 다양한 인증 기술을 지원합니다. 또한 공유 계정에 대한 액세스를 역추적하여 실제 사용자를 확인할 수 있어야 합니다. 시스템 구성 요소에 대한 자동 액세스의 경우 액세스가 시작된 사용자와 작업을 알아야 할 수도 있습니다. CA PAM은 이러한 액세스에 대한 솔루션을 제공합니다. 이러한 시스템 구성 요소에 위험한 액세스를 최소화하기 위해 CA Threat Analytics for PAM은 액세스에 플래그를 표시하여 위험을 더욱 완화합니다.
8.1: 다음과 같이 모든 시스템 구성 요소에서 소비자가 아닌 사용자와 관리자에 대한 올바른 사용자 식별 관리를 보장하는 정책과 절차를 정의하고 구현한다.	CA PAM은 모든 시스템 구성 요소에서 모든 권한 있는 계정의 ID를 관리하기 위한 정책 시행을 지원합니다. 자세한 내용은 아래 8.1.1~8.1.8을 참조하십시오.
8.1.1: 모든 사용자에게 고유한 ID를 배정한 후 시스템 구성 요소나 카드 소지자 데이터에 대한 액세스를 허용한다.	CA PAM은 CA PAM 플랫폼에 고유한 사용자 로그인을 요구한 다음 허가된 시스템 구성 요소에 대한 권한 있는 세션을 설정합니다. 이 구성에서 관리 편의성을 위해 인프라 구성 요소(예: 루트)에 "공유 계정"을 활용할 수 있으며 모든 권한 있는 세션을 추적해 (단순히 IP 주소가 아닌) 특정 개인을 확인할 수도 있습니다.
8.1.2: 사용자 ID, 자격 증명 및 기타 ID 개체의 추가, 삭제, 수정을 제어한다.	CA PAM은 직무 분리를 시행하므로 특별 허가된 관리자만 권한 있는 ID와 기타 자격 증명을 변경할 수 있습니다. 이러한 특별 CA PAM 관리자는 강력한 다단계 인증 방법을 사용해야 하며, 이 세션은 각각 로깅되고 기록됩니다. 이 과정은 CA 아이덴티티 관리 및 거버넌스 솔루션과의 통합으로 더 강화될 수 있습니다.
8.1.3: 권한이 종료된 사용자의 액세스 권한을 즉시 취소한다.	CA PAM을 통해 권한이 종료된 사용자의 모든 시스템 구성 요소에 대한 모든 액세스를 즉시 종료할 수 있습니다.
8.1.4: 최소 90일마다 사용되지 않는 사용자 계정을 삭제/비활성화한다.	CA PAM은 설정한 기간 동안 사용되지 않은 CA PAM 계정을 자동으로 비활성화하는 기능을 지원합니다.

8.1.5: 다음과 같이 시스템 구성 요소를 액세스, 지원 또는 유지 관리하기 위해 공급업체가 원격 액세스로 사용하는 ID를 관리한다. 필요한 기간 중에만 활성화하고 사용하지 않을 때에는 비활성화한다. 사용 시에는 모니터링한다.	CA PAM에서 권한 있는 공급업체 ID 관리 기능은 다른 권한 있는 ID 관리 기능과 동일합니다. 공급업체에 대해서도 시간 제한 액세스를 시행합니다. 또한 각각의 권한 있는 세션을 모니터링하고 기록하며, 정책 위반을 시도할 경우 경보를 보내고 자동으로 액세스를 종료할 수 있습니다.
8.1.6: 6회 이상 로그인을 시도할 경우 사용자 ID를 잠가 반복 액세스 시도를 제한한다.	CA PAM은 관리자가 정의한 횟수 후에 CA PAM 계정을 잠그는 등 실패한 시도 정책을 시행합니다.
8.1.7: 잠금 기간은 최소 30분 또는 관리자가 사용자 ID를 활성화할 때까지로 설정한다.	CA PAM은 허가된 관리자가 계정을 재활성화할 때까지 계정을 잠그는 옵션을 시행할 수 있습니다.
8.1.8: 세션이 15분 넘게 유휴 상태인 경우 사용자에게 터미널 또는 세션을 재활성화하기 위한 재인증을 요구한다.	CA PAM에 세션 제한 시간을 설정할 수 있으며 기본값은 10분으로 설정되어 있습니다.
8.2: 고유한 ID를 배정하는 것 이외에도, 모든 사용자에 대한 인증 방법으로 다음 중 최소한 하나를 사용하여 모든 시스템 구성 요소에서 소비자가 아닌 사용자와 관리자에 대한 적절한 사용자 인증 관리를 보장한다. 사용자가 알고 있는 정보(예: 암호 등). 사용자가 소유하고 있는 기기(예: 토큰 장치나 스마트 카드 등). 사용자의 신체 일부(예: 생체 인식 등).	CA PAM은 강력한 다단계 인증 시스템을 포함한 다양한 인증 방법과의 통합을 지원합니다. 이 솔루션은 선택한 인증 시스템(예: AD, RADIUS, 스마트 카드)에 인증 요청을 전달합니다. 성공적으로 인증되면 CA PAM은 CA PAM의 개인 또는 그룹 정책을 기준으로 명시적으로 액세스가 허가된 리소스 및 사용할 수 있는 액세스 방법의 목록을 사용자에게 제공합니다. 이러한 방식으로 인증과 허가를 분리할 수 있습니다.
8.2.1: 강력한 암호화를 사용하여 모든 인증 자격 증명(예: 암호 등)을 모든 시스템 구성 요소에서 전송 및 저장되는 동안 읽을 수 없도록 한다.	CA PAM은 암호와 기타 인증 자격 증명을 암호화된 금고에 저장하고, 모든 암호화 작업에 FIPS 140-2 보안 커널을 사용합니다. 하드웨어 보안 모듈(HSM)과 통합하면 더 높은 수준으로 FIPS 140-2 규정 준수를 달성할 수 있습니다. 암호와 기타 자격 증명은 보안/암호화 채널을 통해 전송됩니다.
8.2.2: 암호 재설정을 수행하거나 새 토큰을 프로비저닝하거나 새 키를 생성하는 등 인증 자격 증명을 수정하기 전에 사용자 ID를 검증한다.	인증이 성공해야 암호 재설정 사용, 새 암호화 키 생성 등의 작업을 할 수 있도록 CA PAM을 구성할 수 있습니다.
8.2.3: 암호는 다음 조건을 충족해야 한다. 최소 길이는 7자이다. 숫자와 알파벳을 둘 다 포함한다. 또는 암호의 복잡도와 강도가 위에 지정한 매개 변수 이상이어야 한다.	CA PAM은 최소 암호 길이와 서로 다른 유형의 문자 사용을 포함한 업계 표준 암호 길이 및 강도/조합 정책을 시행합니다.

8.2.4: 최소 90일마다 사용자 암호를 변경한다.	CA Privileged Access Manager는 임의의 시간 간격으로 암호 변경을 시행합니다. 시스템의 암호 관리 기능에서 시스템에 설정된 정책에 따라 자동으로 변경을 수행합니다.
8.2.5: 최근에 사용한 4개의 암호 중 하나를 새 암호로 제출하는 것을 허용하지 않는다.	CA PAM은 업계 표준에 따른 완전히 구성 가능한 암호 재사용 정책을 시행하며, 암호를 재사용하는 데 필요한 반복 횟수, 암호 사용 일수 등의 관리자가 결정하는 설정이 포함됩니다.
8.2.6: 최초 사용 및 재설정 시 사용자별 고유한 값으로 암호를 설정하고 첫 사용 직후에 변경한다.	CA PAM은 암호 조합, 재사용, 수명을 포함한 포괄적인 암호 정책을 구현합니다. 일회용 암호를 지원하며 일회용 암호 사용 후에는 새 암호를 자동으로 설정하도록 구성할 수도 있습니다. 또 다른 옵션은 암호 만료 기간을 두는 것으로 암호의 유효 기간을 자동으로 설정합니다.
8.3: 다단계 인증을 사용하여 모든 개별 비 콘솔 관리 액세스 및 CDE에 대한 모든 원격 액세스를 보호합니다.	CA Privileged Access Manager는 다양한 다단계 인증 방법을 지원하며 RADIUS 및 X.509 인증서와 스마트 카드를 지원합니다. CA Privileged Access Manager는 권한 있는 사용자가 허가된 리소스에 액세스할 수 있도록 설정하기 전에 강력한 다단계 인증을 시행할 수 있습니다. 또한 업계 최고의 CA 고급 인증 기능을 통합하여 다단계 인증을 시작할 수도 있습니다. PAM의 Threat Analytics를 통해 권한 있는 사용자의 행동이 정상적이 아닌 경우 해당 세션을 종료할 수 있습니다. 다단계 인증은 다음 로그인 시 강제로 시행될 수 있습니다.
8.3.1: 개인(사용자와 관리자 포함)과 모든 제3자(지원이나 유지 관리를 위한 공급업체 액세스 포함)가 네트워크 외부에서 원격 네트워크에 액세스하는 경우 다단계 인증을 적용한다.	CA PAM은 다양한 다단계 인증 방법과 RADIUS, X.509 인증서 및 스마트 카드를 지원합니다. CA PAM은 권한 있는 사용자가 허가된 리소스에 액세스할 수 있도록 설정하기 전에 강력한 다단계 인증을 시행할 수 있습니다. 또한 업계 최고의 CA 고급 인증 기능을 통합하여 다단계 인증을 시작할 수도 있습니다. CA Threat Analytics for PAM을 통해 권한 있는 사용자의 행동이 정상적이 아닌 경우 해당 세션을 종료할 수 있습니다. 다단계 인증은 다음 로그인 시 강제로 시행될 수 있습니다.

8.5: 다음과 같이 그룹, 공유 또는 일반 ID, 암호, 기타 인증 방법을 사용하지 않는다. • 일반 사용자 ID는 비활성화하거나 제거한다. • 시스템 관리와 기타 중요한 기능에 공유 사용자 ID를 사용하지 않는다. • 시스템 구성 요소 관리에 공유 및 일반 사용자 ID를 사용하지 않는다.	기존 구성에서 공유 계정의 문제는 누가 무엇을 했는지 알 수 없다는 것입니다. 누구나 루트 또는 관리자로 로그인한다면 각 권한 있는 사용자가 사실상 익명화됩니다. 그러나 공유, 일반, 그룹 계정은 특히 대규모 네트워크에서 시스템 구성 요소의 구성과 관리를 크게 간소화합니다. CA PAM을 사용하면 양쪽의 장점만 취하여 공유 계정을 완전히 귀속된(검증 가능한) 방식으로 사용할 수 있습니다. 조직은 공유 계정을 사용하는 서버, 네트워크 장치, 기타 구성 요소를 구성할 수 있지만, 정확히 누가 공유 계정에 로그인했고 정확히 무엇을 했는지 구체적이고 검증 가능한 기록을 얻을 수 있습니다. 이러한 공유 계정의 암호는 CA PAM 금고에 저장되므로 사용자는 CA PAM에 로그인해야만 공유 계정 액세스 권한을 받게 됩니다. 사용자가 공유 계정에 로그인하면 CA PAM이 모든 사항을 모니터링하고 기록하므로, 권한 있는 사용자가 공유 계정을 사용하여 수행한 활동을 역추적하여 특정 사용자를 확인할 수 있습니다.
8.6: 다른 인증 메커니즘을 사용하는 경우(예: 물리적 또는 논리적 보안 토큰, 스마트 카드, 인증서 등) 이러한 메커니즘 사용을 다음과 같이 지정해야 한다. 인증 메커니즘은 개별 계정에 지정해야 하며 여러 계정이 공유해서는 안 된다. 의도한 계정만 해당 인증 메커니즘을 사용하여 액세스할 수 있도록 물리적 및/또는 논리적 제어를 마련해야 한다.	CA PAM은 보안 토큰, 스마트 카드 및 디지털 인증서를 포함하여 다양한 인증 메커니즘 사용을 지원합니다. 각 메커니즘은 개별 고유 ID에 지정할 수 있으며 추가 인증 메커니즘을 병용하여 허가된 사람만 보안 토큰, 스마트 카드 또는 디지털 인증서를 통해 액세스할 수 있도록 지원합니다.
8.7: 카드 소지자 데이터가 있는 데이터베이스에 대한 모든 액세스(애플리케이션, 관리자, 다른 모든 사용자의 액세스 포함)는 다음과 같이 제한한다. 데이터베이스에 대한 모든 사용자 액세스, 사용자 쿼리, 사용자 작업은 프로그래밍 방식을 통한다. 데이터베이스 관리자만 데이터베이스에 직접 액세스하거나 쿼리할 수 있다. 데이터베이스 애플리케이션용 애플리케이션 ID는 (개별 사용자나 다른 비 애플리케이션 프로세스가 아닌) 애플리케이션만 사용할 수 있다.	CA PAM은 허가된 관리자만 카드 소지자 데이터베이스에 직접 액세스할 수 있도록 제한합니다. 또한 애플리케이션만 사용할 수 있는 애플리케이션 계정을 제공합니다.
10.1: 시스템 구성 요소에 대한 모든 액세스를 각 개별 사용자와 연결하도록 감사 내역을 구현한다.	CA PAM은 모든 권한 있는 액세스를 특정 사용자와 연결합니다. 강력한 다단계 인증을 지원하여 허가된 개인만 권한 있는 계정을 사용하여 시스템 구성 요소에 액세스할 수 있으므로, 각각의 권한 있는 세션을 허가된 사용자에게 명확하게 귀속시킬 수 있습니다.
10.2: 모든 시스템 구성 요소에 대해 다음 이벤트를 재구성하는 자동화된 감사 내역을 구현한다.	권한 있는 사용자가 서버, 데이터베이스, 네트워크 장치, 애플리케이션 등 시스템 구성 요소에서 수행하는 모든 작업은 CA PAM이 변조 방지 로그(Tamper-Evident Log)에 기록하며 이 로그는 명확하게 허가된 개인만 액세스하고 검토할 수 있습니다. 자세한 내용은 아래 10.2.1~10.2.7을 참조하십시오.

10.2.1: 카드 소지자 데이터에 대한 모든 개별 사용자 액세스	카드 소지자 데이터베이스에 대한 허가된 데이터베이스 관리자 액세스와 같은 모든 관리자 액세스는 CA PAM이 모니터링하고 기록합니다.
10.2.2: 루트 또는 관리 권한으로 개인이 수행한 모든 작업	CA PAM은 모든 권한 있는 활동을 모니터링하고 기록합니다. 조직이 공유된 관리 계정을 사용하는 경우에도 CA PAM은 수행된 각 작업을 고유한 사용자에게 명확하게 귀속시킬 수 있습니다.
10.2.3: 모든 감사 내역에 대한 액세스	CA PAM은 직무 분리 기능을 제공하므로 특별 허가된 사용자만 CA PAM 로그 파일과 기록을 검토할 수 있습니다. 허가된 사용자가 로그를 검토할 때마다 그 사실 역시 로깅되고 기록될 수 있습니다.
10.2.4: 잘못된 논리적 액세스 시도	CA PAM은 CA PAM 플랫폼을 통해 발생한 모든 잘못된 논리적 액세스 시도를 추적합니다. 우선, 허가된 사용자만 CA PAM에 액세스할 수 있으며 일단 액세스하면 명시적으로 허가된 시스템에만 액세스할 수 있습니다. 허가된 시스템에 액세스한 후에도 CA PAM은 허가된 시스템을 사용하여 허가되지 않은 시스템에 액세스하려는 시도(립프로깅(Leapfrogging)이나 RDP 호핑)를 방지할 수 있습니다. CA PAM은 플랫폼 외부에서 시도한 로그인 실패(예: 서버에 직접 연결하고 로그인하려는 시도)는 로깅하지 않습니다. 그러나 모든 암호/자격 증명이 CA PAM 금고에 저장되고 사용자는 암호를 알 수 없으므로 CA PAM 플랫폼을 통하지 않고서는 시스템에 로그인할 방법이 없습니다.
10.2.5: 식별 및 인증 메커니즘의 사용 및 변경 (새 계정 생성과 권한 상승 등 다양한 작업) 그리고 루트 또는 관리 권한이 있는 계정의 모든 변경, 추가, 삭제	CA PAM은 권한 있는 계정의 모든 식별 및 인증 활동을 로깅하며 여기에는 계정에 관련된 모든 변경 사항과 계정의 모든 사용 내역이 포함됩니다.
10.2.6: 감사 로그의 시작, 중지 또는 일시 중지	CA PAM은 로깅이 시작되었음을 표시하는 로그 항목이 없지만 기본적으로 끊임없이 로그를 생성합니다.
10.2.7: 시스템 수준 개체의 생성과 삭제	CA Privileged Access Manager에서 허가된 관리자는 대상 서버, 계정, 암호, 그룹, 사용자 등을 생성하고 삭제할 수 있습니다.
10.3: 최소한 각 이벤트에 대해 모든 시스템 구성 요소의 다음 감사 내역 항목을 기록한다.	CA PAM은 모든 시스템 구성 요소에 대한 권한 있는 액세스의 완전한 감사 내역을 기록합니다. 자세한 내용은 10.3.1~10.3.6에 대한 아래 대응을 참조하십시오.

10.3.1: 사용자 식별	사용자는 강력한 다단계 방법을 통해 인증되므로 CA PAM이 유지 관리하는 로그와 기록에 고유한 사용자가 캡처됩니다.
10.3.2: 이벤트 유형	CA PAM syslog 이벤트는 로그인/로그아웃 시도, 정책 위반 시도, 원격 세션 설정 등으로 분류됩니다.
10.3.3: 날짜와 시간	날짜와 시간은 syslog 및 세션 기록 스트림의 일부로 캡처됩니다.
10.3.4: 성공 또는 실패 표시	CA PAM은 로그인/로그아웃 시도와 같이 성공 또는 실패가 결정되는 이벤트마다 성공 또는 실패를 로깅합니다.
10.3.5: 이벤트 발생 지점	CA PAM은 각 이벤트를 위해 솔루션에 액세스하는 데 사용된 고유한 사용자 ID와 소스 IP 주소를 캡처합니다.
10.3.6: 영향받는 데이터, 시스템 구성 요소 또는 리소스의 ID나 이름	시스템 구성 요소, 리소스 등에 영향을 주는 이벤트의 경우 영향받는 대상의 ID(예: 호스트 이름)와 시스템에 액세스하는 사용자가 캡처됩니다.
10.4: 시간 동기화 기술을 사용하여 모든 중요 시스템 시계와 시간을 동기화하고 시간을 획득, 배포, 저장하기 위해 다음 사항을 구현한다.	CA PAM은 업계 표준 시간 동기화 기술인 NTP(Network Time Protocol)를 지원합니다.
10.4.1: 중요 시스템에 정확하고 일관된 시간을 적용한다.	CA PAM은 NTP를 사용하여 시간 동기화를 수행하고 감사 로그와 기록에 정확하고 일관된 타임스탬프를 적용합니다.
10.4.2: 시간 데이터를 보호한다.	인증된 NTP를 사용하여 기본 NTP보다 무결성 수준을 높이도록 CA PAM을 구성할 수 있습니다.
10.4.3: 업계에서 인정하는 시간 소스에서 시간 설정값을 받는다.	2개의 기본 시간 서버가 지정되어 있으며 허가된 CA PAM 관리자가 추가 및/또는 변경할 수 있습니다.
10.5: 감사 내역을 변경할 수 없도록 보호한다.	CA PAM 로그와 기록은 무단 액세스와 수정으로부터 보호되며 발생하는 모든 변경 사항이 감지됩니다.
10.5.1: 감사 내역 열람을 업무상 필요한 사람으로 제한한다.	CA PAM 로그와 기록은 최소 권한 원칙과 역할 기반 액세스 제어에 따라 명시적으로 허가된 직원만 액세스할 수 있습니다.

10.5.2: 감사 내역 파일을 무단 수정으로부터 보호한다.	모든 CA PAM 로그와 기록은 암호화 해싱(Hashing) 기법을 사용하여 변조 방지됩니다. CA PAM은 파일이 변조되면 알립니다.
10.5.3: 감사 내역 파일은 중앙 로그 서버나 변경하기 어려운 미디어에 즉시 백업한다.	CA PAM은 syslog 전달 기능을 제공하므로 모든 CA PAM 로그를 중앙 syslog 서버, 1회 쓰기 미디어, 기타 형태의 로그 스토리지 및 보관소에 백업할 수 있습니다.
10.5.5: 로그에 파일 무결성 모니터링 또는 변경 탐지 소프트웨어를 사용하여 기존 로그 데이터가 변경되면 경보가 발생하도록 한다. 물론 데이터가 새로 추가되는 경우에는 경보가 발생해서는 안 된다.	CA PAM 로그와 기록은 암호화 해싱 기법을 사용하여 변조 방지됩니다. 새 데이터의 표준적인 추가가 아닌 기존 로그나 기록의 수정은 탐지됩니다.
10.6(10.6.1~10.6.3 포함): 모든 시스템 구성 요소의 로그와 보안 이벤트를 검토하여 이상 징후 또는 의심스러운 활동을 식별한다.	CA Threat Analytics for PAM은 강력한 머신러닝 기반의 UBA(User-Behavior-Analytics) 솔루션을 제공합니다. 이 솔루션은 SIEM 솔루션 및 다른 엔터프라이즈 로깅 솔루션과 함께 작동하며 사용자 기반 활동과 관련된 위험을 판별하는 데 사용될 수 있습니다. 판별된 위험은 다양한 기법을 사용하여 완화할 수 있습니다.
10.7: 감사 내역은 최소 1년간 보존하고 최소 3개월간은 분석에 즉시 사용할 수 있도록 한다(예: 온라인, 보관 또는 백업에서 복원 가능).	CA PAM은 syslog를 사용하므로 필요한 기간 동안 감사 내역을 syslog 서버에 보관할 수 있습니다. 이렇게 하면 로그 데이터를 분석에 즉시 사용할 수 있으면서도 로컬 CA PAM 시스템의 여유 스토리지 공간을 확보하게 됩니다. 로컬 CA PAM 시스템은 로그를 4개월 동안 보존할 수 있습니다.
12: 모든 직원에 대한 정보 보안을 다루는 정책 유지 관리	CA PAM을 통해 조직은 카드 소지자 데이터를 보호하는 권한 있는 사용자 정책을 캡처하고 시행할 수 있습니다. 카드 소지자 데이터 처리에 관련된 각 시스템 구성 요소에 필요한 제어가 마련되어 있다는 것을 매우 쉽게 입증할 수 있습니다.
12.2: 다음과 같은 위험 평가 프로세스를 구현한다. 최소 매년 그리고 중대한 환경 변화(예: 인수, 합병, 재배치 등)가 발생할 시 수행한다. 중요 자산, 위협, 취약점을 식별한다. 공식적인 위험 평가 결과를 보고한다.	CA PAM을 통해 조직은 로그와 기록을 검토할 수 있습니다(DVR 형식의 재생 사용). 모든 정책 위반 시도가 로깅되므로 정책 위반 시도가 발생한 관리 세션을 집중적으로 검토한 다음 다른 세션에 이상한 점이 없는지 부분적으로 검사할 수 있습니다.

섹션 3

결론

PCI DSS 버전 3.2 규정이 2018년 2월부터는 필수 사항이 되므로 조직에서는 지속적인 규정 준수를 지원하는 확장 가능한 솔루션을 고려하는 것이 중요합니다. 이를 위해 다음 요소를 고려할 필요가 있습니다.

- **확장성 및 고가용성.** PCI DSS 범위에 포함되는 시스템과 애플리케이션이 민감한 카드 소지자 데이터를 보유하고 있는 경우, 애플리케이션뿐만 아니라 애플리케이션을 보호하는 솔루션도 고가용성이어야 합니다. 따라서 권한 있는 액세스 관리 솔루션은 사용자와 사용자 액세스에 대한 인증, 허가뿐만 아니라 세션 관리와 기록에서도 확장성이 높아야 합니다.
- **범위 확장성.** 비즈니스 성장이나 구축 단계에 따라 더 많은 시스템과 애플리케이션이 PCI DSS에 포함될 수 있으므로, 권한 있는 액세스 관리 솔루션은 새로운 인프라와 애플리케이션을 신속하고 효율적으로 포함하도록 쉽게 범위를 확장할 수 있어야 합니다. 또한 사용자, 시스템 및 애플리케이션 수가 급증하면 사용자 활동의 수동 모니터링이 어려워집니다. 권한 있는 액세스 솔루션은 분석 기반 위험 완화 전략을 제공해야 합니다. 포괄적인 표준 지원을 제공하기 위해서는 권한 있는 액세스 관리를 다른 솔루션과 통합할 필요성이 높으며 이는 중요한 고려 사항입니다.
- **소유 비용.** 권한 있는 액세스 관리 솔루션의 필수 기능이 늘어나면서 일정 기간(일반적으로 3~5년) 동안의 소유 비용이 너무 높아서는 안 됩니다. 예를 들어, 권한 있는 액세스 관리 솔루션은 암호 보관 기능만으로 쉽게 시작할 수 있지만 PCI DSS는 암호 정책, 허가, 세션 관리 및 기록과 같은 기능을 비롯하여 그 이상의 기능과 정책을 요구합니다. 이런 기능이 별도로 제공되는 경우 조직은 인프라, 기술 세트와 라이선싱뿐 아니라 단계별 구축 비용도 고려해야 할 수 있습니다. 또한 유지 관리 및 통합 비용은 단계별로 다를 수 있으며 초기 단계의 낮은 진입 가격을 향후 단계에서는 적용하기 어려워집니다.

CA 권한 있는 액세스 관리 솔루션의 이점을 알아보려면 **ca.com/pam**을 방문하십시오.

CA 테크놀로지스에 연결

CA 테크놀로지스(NASDAQ: CA)는 회사가 혁신을 통해 애플리케이션 경제의 기회를 잡을 수 있도록 하는 소프트웨어를 만듭니다. 소프트웨어는 모든 업종, 모든 기업의 핵심 요소입니다. 계획부터 개발, 관리 및 보안에 이르기까지 CA는 전 세계 기업들과 함께 모바일, 프라이빗 및 퍼블릭 클라우드, 분산 및 메인프레임 환경에서 생활, 거래, 소통의 방식을 바꾸고 있습니다. 자세한 내용은 ca.com/kr을 참조하십시오.

CS200-298517_0817