제공:

thycotic

초보자를 위한 특권 계정 관리

for dummies®
A Wiley Brand

특권 계정 관리(PAM)의 이해

PAM 보안 솔루션 개발

조직을 보호하는 주요 방법

Joseph Carson, CISSP

Thycotic 스페셜 에디션

Thycotic 소개

IT 보안 분야의 글로벌 선도 기업인 Thycotic은 가장 빠르게 성장하고 있는 특권 계정 관리 솔루션 제공업체입니다. 특권 계정 관리 솔루션은 조직의 가장 가치 있는 자산을 사이버 공격과 내부 위협으로부터 보호합니다. Thycotic은 Fortune 선정 500대 기업을 포함하여 전 세계 7,500개 이상의 조직을 위해 특권 계정 액세스 보안을 지원하고 있습니다. 수상 경력에 빛나는 Thycotic의 특권 계정 관리 보안 솔루션(Privileged Account Management Security solution)은 특권 자격 증명의 위험을 최소화하고 사용자 권한을 제한하며 엔드포인트와 서버에서 애플리케이션을 통제합니다. 1996년에 설립된 Thycotic은 워싱턴 D.C.에 본사를, 영국과 호주에 글로벌 사무소를 두고 있습니다. 자세한 내용은 www.thycotic.com에서 확인할 수 있습니다.

초보자를 위한

특권 계정 관리

Thycotic 스페셜 에디션

저자: Joseph Carson, CISSP

for dummies®
A Wiley Brand

Privileged Account Management For Dummies®, Thycotic 스페셜 에디션

출판사:
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN: 978-1-119-38684-1 (pbk); ISBN: 978-1-119-38685-8 (ebk)

미국에서 제작됨

10 9 8 7 6 5 4 3 2 1

출판에 도움을 주신 분들

이 책이 출판되는 데 도움을 주신 분들은 다음과 같습니다.

프로젝트 에디터: Carrie A. Burchfield
편집장: Rev Mengle
원고 검토 에디터: Amy Fandrei
비즈니스 개발 담당자: Ashley Barth
프로덕션 에디터: Antony Sami

서론

외부 공격자와 악의적인 내부자에 의한 정교한 보안 위협이 증가함에 따라, 조직이 중요하고 민감한 정보를 적절하게 보호하는 일이 매우 어려워졌습니다. 설상가상으로, IT 환경이 더 복잡해지고 여러 지리적 위치와 클라우드로 분산되면서 이러한 자산을 보호하는 일은 더욱더 어려워지기만 합니다.

최근 주목의 대상이 된 많은 침해 사건은 한 가지 공통점이 있습니다. 그 공통점은 바로 비밀번호가 노출되어 발생했다는 점입니다. 많은 경우, 최종 사용자의 비밀번호는 다양한 사회 공학 기법에 의해 최초로 해킹됩니다. 그런 다음에, 권한이 승격되어 보다 많은 권한을 주는 계정에 액세스할 수 있게 됩니다. 왕국으로 가는 열쇠를 얻게 되는 셈입니다. 이러한 무단 액세스는 몇 주 또는 심지어 몇 개월 동안 탐지되지 않을 수 있어서, 이 기간 동안 해커는 자신의 편의대로 정보를 열람하고 훔칠 수 있습니다.

안타깝게도, 특권 계정이 기능하는 방식과 이 계정이 침해되거나 오용될 경우 발생하는 위험을 완전히 이해하지 못하는 IT 사용자가 많습니다. 사정이 이렇다 보니, IT 사용자와 조직은 증가하는 위협으로 인한 잠재적인 금전적 피해와 평판 훼손에 더욱 취약해집니다.

이 책 소개

IT 전문가의 경우, 이 책을 통해 특권 계정 관리(privileged account man-agement, PAM)를 실질적으로 이해할 수 있습니다. 이 책은 특권 계정이 무엇이고 IT 환경 어디에 존재하며 어떻게 기능하는지에 대해 설명합니다. 가장 중요한 것은 이 책이 특권 계정과 관련된 위험과 이러한 계정을 해커와 악의적인 내부자가 가하는 위협으로부터 보호하는 방법을 설명한다는 점입니다.

이 책은 조직을 보안 위협으로 보호하는 일을 담당하는 IT 관리자, 시스템 관리자, 보안 전문가를 위해 작성되었으며, 독자가 IT 네트워크 관리와 관련된 기본적 IT 전문 지식과 경험을 보유하고 있고 일상적인 업무를 위해 특권 계정과 비밀번호를 사용한다는 것을 전제로 합니다.

그러나, 특권 계정 보안 지침의 중요성에 관해 알아보려는 비즈니스 사용자와 기타 사용자에게도 이 책이 유용할 수 있습니다.

이 책에서 사용되는 아이콘

이 책에서는 특별한 콘텐츠를 표시하기 위해 다음과 같은 아이콘을 사용합니다.


기억할 사항

이 정보를 기억해야 합니다. 이 정보는 PAM 프로세스를 기본적으로 이해하는 데 꼭 필요합니다.


기술적 정보

IT 관리자와 시스템 관리자가 관심을 가질 만한 보다 기술적인 정보를 나타냅니다.


팁

특권 계정 비밀번호 보안 전략을 수립할 때 시간과 노력을 절약해 줄 실용적인 조언을 표시합니다.


경고

주의하십시오! 여기에 제시된 세부 정보에 면밀한 관심을 기울이십시오. 이 정보는 여러분과 조직의 보안에 중대한 영향을 주는 심각한 문제에 대해 알려줍니다.

더 자세한 정보를 얻으려면

PAM과 비밀번호 보안에 대한 더 자세한 정보를 원하는 IT 전문가는 Thycotic의 웹사이트 www.thycotic.com에서 자세한 내용을 확인할 수 있습니다.

Resources 링크에는 Windows 및 Unix 플랫폼에서 비밀번호 취약점을 찾아내는 여러 가지 무료 툴과 함께 무료 보안 정책, Weak Password Finder Tool, 온라인 보안 교육, PAM 및 전반적인 보안 관행의 유효성을 측정하는 데 도움이 되는 벤치마킹 툴이 포함되어 있습니다.

이 장의 내용

» 특권 계정과 사용자 계정 구분

» 특권 계정의 유형 이해

» 특권 계정 비밀번호 관리 및 보호

1장 특권 계정 관리에 대해 알아보기

특권 계정은 IT 환경 어디에서나 사용됩니다. 특권 계정은 정보 중심의 세상을 뒷받침하는 하드웨어와 소프트웨어로 구성된 대규모의 네트워크를 관리할 수 있는 구성 요소를 IT 부서에 제공합니다. 그러나, 대부분의 사람들은 특권 계정을 볼 수 없습니다.

이 장에서는 특권 계정 관리(PAM)의 기초, 즉 특권 계정과 이 계정이 하는 일, 확장일로에 있는 정보의 세계에서 "왕국으로 가는 열쇠"인 특권 계정에 대한 액세스를 보호하는 일이 중요한 이유 등을 설명합니다.

특권 계정 이해하기

계정은 크게 두 가지 카테고리로 나눌 수 있습니다. 사용자 계정은 사람이 사용하는 온라인 뱅킹 또는 쇼핑몰 계정과 같은 형태를 띱니다. 모든 사용자 계정은 비밀번호가 있으며 이 비밀번호로 사용자는 계정에 액세스하고 작업을 수행합니다. 비밀번호는 사용자의 허가 없이 다른 누군가가 사용자 계정에 액세스하지 못하도록 하여 정보를 보호합니다.

사용자 계정과 특권 계정 비교

일반적으로 사용자 계정은 Active Directory 사용자 계정과 같이 개인의 ID를 나타내며 비밀번호가 연결되어 있어 해당 계정에 대한 액세스를 제한합니다. 보통 한 사람의 사용자당 한 개의 계정 비밀번호가 있으며 이 사람은 이 비밀번호를 기억해야 합니다.

특권 계정(privileged account)은 사람일 수도 있고 사람이 아닐 수도 있으며, 반드시 사람을 대표하는 것은 아닙니다. 그 예로는 **IT 직원들이 흔히 공유하는 애플리케이션 계정**이 있습니다. **특권 계정의 비밀번호**는 길고 복잡한 값으로 설정해야 하며 안전한 곳에 보관해야 합니다. 올바르게 보관한다면 이러한 계정은 기억할 필요가 없습니다.

*특권 계정*은 사람일 수도 있고 사람이 아닐 수도 있습니다. 특권 계정은 IT 전문가가 애플리케이션, 소프트웨어, 서버 하드웨어를 관리하도록 지원하기 위해 존재합니다. 특권 계정은 공유되는 더 높은 수준의 권한을 바탕으로 관리자 수준의 액세스 또는 전문적 수준의 액세스를 제공합니다. 사람이 아닌 것을 대표하는 특권 계정의 유형으로는 구체적인 권한을 요구하는 서비스를 실행하는 데 사용되는 애플리케이션 계정이 있습니다. 많은 경우, 사용자 계정에도 승격된 특권, 또는 관리자 특권이 추가될 수 있습니다.


경고

사용자 계정과 마찬가지로 특권 계정에도 액세스 제어를 위한 비밀번호가 있습니다. 사용자 및 특권 계정 비밀번호와 관련된 문제는 해커가 이러한 비밀번호를 크래킹(cracking)하도록 돕는 많은 툴이 존재한다는 점입니다. 해커가 비밀번호로 보호되는 시스템에 액세스할 수 있게 되면 치명적인 피해가 발생할 수 있습니다. 특권 계정을 가로채면 공격자는 조직의 가장 민감한 데이터에 액세스하고 이를 다운로드할 수 있으며, 맬웨어를 배포하고, 기존 보안 제어 조치를 우회하고, 활동을 숨기기 위해 감사 트레일을 지울 수 있습니다.

대부분의 조직에서 IT 직원은 표준 권한이 부여된 계정과 승격된 권한이 필요한 작업을 수행하기 위한 계정을 별도로 가지고 있습니다. 다양한 유형의 특권 계정인 IT 계정의 예는 아래와 같습니다.

- 서버를 관리하는 로컬 또는 도메인 관리자 계정
- 일반적으로 Active Directory 사용자를 제어하는 도메인 관리자 계정

- 데이터베이스 관리를 지원하는 시스템 관리자 계정인 SA 계정
- Unix/Linux 플랫폼을 관리하는 루트 계정
- Windows 애플리케이션, 서비스, 예약된 작업을 실행하고 관리하는 계정
- IIS 애플리케이션 풀(.NET 애플리케이션)
- 방화벽, 라우터, 스위치에 대한 액세스 권한을 부여하는 네트워킹 장비 계정

특권 계정 유형의 한 예는 작업 또는 애플리케이션을 실행하고 예약하기 위한 특별 권한을 요구하는 서비스 계정입니다. 이러한 계정은 일대다 방식으로 사용되는 경우가 많습니다. 즉, 하나의 계정을 여러 서비스 또는 애플리케이션을 실행하기 위해 조직 전체에서 사용할 수 있습니다.


경고

안타깝게도, 서비스 계정은 오용되는 경우가 많습니다. 운영을 지속하고 애플리케이션 가동중단시간(downtime) 또는 권한이 불충분해지는 경우를 방지하기 위해, 서비스 계정은 높은 수준의 권한과 절대로 변경되거나 만료되지 않는 비밀번호로 구성하는 경우가 많습니다. 이러한 일반적인 관행은 어느 조직에게나 위험한 취약성을 유발합니다.

특권 계정을 사용하는 사람과 특권 계정의 위치

대표적인 특권 계정 사용자는 환경 관리를 담당하는 시스템 관리자(sysadmin) 또는 특정 소프트웨어나 하드웨어를 담당하는 IT 관리자입니다. 이들은 다음과 같은 작업을 수행합니다.

- 시스템 하드웨어/소프트웨어 설치
- 민감한 데이터에 액세스
- 다른 사람을 위해 비밀번호 재설정
- 환경 내의 모든 시스템에 로그인
- IT 인프라 시스템을 변경하기 위해 승격된 권한 사용

특권 계정은 IT 시스템 배포 및 유지보수를 위해 시스템 관리자가 사용하므로 연결된 거의 모든 디바이스, 서버, 데이터베이스, 애플리케이션에 존재합니다. 또한, 특권 계정은 조직의 기존 IT 인프라 밖으로 확장되어 직원이 관리하는 기업 소셜 미디어 계정도 포함할 수 있습니다.

따라서, 조직은 일반적으로 직원보다 두세 배 더 많은 특권 계정을 갖고 있습니다. 많은 경우, 조직 내 특권 계정 중 일부는 알려지지 않아서 관리되지 않기 때문에 보호받지 못할 수 있습니다.

특권 계정이 해커들의 주요 표적이 되는 이유

업계 분석가들은 현재 모든 보안 침해 사례의 60~80%가 사용자 및 특권 계정 비밀번호에 대한 침해인 것으로 추정하고 있습니다. 그러나, 특권 계정을 확인하고 관리하기 위한 기존의 방법은 여전히 드물게 또는 임시적으로 수행하는, 시간이 많이 드는 수작업에 의존하고 있습니다.

심지어 최첨단 IT 환경에서조차 특권 계정에 대해 여러 시스템에서 공통 비밀번호를 사용하고 자격 증명을 무단으로 공유하며 비밀번호 기본값을 변경하지 않은 채 사용하는 경우가 많습니다. 이 때문에 특권 계정은 공격의 주요 표적이 됩니다.

대부분의 공격자에게 낮은 레벨의 사용자 계정을 확보하는 일은 첫 단계에 불과하므로, 이러한 관행으로 인해 쉽게 보안이 침해될 수 있습니다. 공격자의 실제 목표는 특권 계정을 확보하여 애플리케이션, 데이터, 주요 관리 기능에 대한 액세스 권한을 승격하는 것입니다. 특권 계정 자격 증명에 액세스 권한을 얻으면 해커는 정당한 관리 사용자로 위장하여 자신의 활동을 쉽게 숨길 수 있습니다.

2장에서는 공격자가 어떻게 사용자 및 특권 계정 비밀번호를 알아내는지와 이러한 활동을 방지하기 위해 할 수 있는 일에 대해 알아보겠습니다.

이 장의 내용

- 사이버 범죄자가 특권 계정 비밀번호를 알아내는 방법 이해하기
- 특권 계정이 해킹될 경우 일어나는 일 살펴보기
- 기존의 IT 보안 방법만으로는 부족한 이유 알아보기

2장
특권 계정이 침해될 경우 발생하는 위험 살펴보기

특권 계정은 어느 IT 환경에서나 비즈니스 운영을 위해 저장되고 사용되는 민감한 정보에 특별한 액세스 권한을 부여하는 "왕국으로 가는 열쇠"입니다. 특권 계정을 한 번만 침해해도 공격자는 조직의 IT 네트워크 내에 있는 거의 모든 정보에 액세스할 수 있습니다.

공격자가 특권 계정을 확보하게 되면 악의적 활동을 수행하고 민감한 정보를 훔치며 금융 사기를 저지르고 한 번에 몇 주 또는 몇 개월씩 탐지를 피할 수 있습니다. 대부분의 사이버 보안 침해 사건은 200일 이상 탐지를 피했습니다.

위험은 명백하게 드러나지만, 사이버 범죄자와 악의적 내부자가 어떻게 최종 사용자 또는 특권 계정을 침해하고 권한을 "승격"하여 정보를 훔치고 조직의 평판을 훼손하는지를 이해하는 것이 중요합니다.

사이버 범죄자가 특권 계정을 침해하는 방법

침해 사건의 최대 80%가 도난당하거나 취약한 비밀번호 자격 증명 때문에 발생하고 있으며, 특권 계정 침해 경로는 상당히 간단합니다. 해커가 가장 선호하는 특권 공격 경로는 아래와 같습니다.

1. **최종 사용자 계정 침해.**

   해커들은 맬웨어 또는 사회 공학을 이용하여 데스크탑, 노트북 또는 서버에 액세스합니다. 일반적으로 직원들이 속아서 맬웨어가 숨겨진 링크를 클릭하거나 소프트웨어를 다운로드하거나 가짜 웹사이트에 비밀번호 자격 증명을 입력하도록 요구하는 피싱 사기에 걸려듭니다. 많은 경우, 이러한 사기는 직원의 매니저, 회사 임원 또는 다른 신뢰할 수 있는 소스에서 보낸 정당한 요청처럼 보입니다.

2. **특권 계정 캡처.**

   공격자가 자유롭게 돌아다니려면 특권 계정(로컬 Windows 관리자/서비스 계정)이 필요합니다. 직원의 비밀번호를 사이버 범죄자가 포착하면 공격자는 네트워크에 로그온하여 많은 기존 IT 보안 제어 조치를 우회할 수 있습니다. 이들은 정당한 자격 증명을 가진 사용자처럼 *보이기* 때문입니다. 해커가 가장 흔히 사용하는 기법은 권한을 승격하기 위한 Man in the Middle 또는 Pass the Hash 공격입니다.

3. **네트워크의 모든 곳에 액세스.**

   특권 자격 증명이 있으면 해커는 **핵심 네트워크 서비스에 액세스하여 몇 주 또는 몇 개월 동안 탐지를 피하면서** 맬웨어를 퍼뜨리거나 가치 있는 정보를 훔칠 수 있습니다.

경고

사이버 범죄자는 또한 비밀번호 기본값을 변경하지 않은 최종 사용자 또는 특권 계정을 침해할 수 있습니다. 예를 들면, 최근 Thycotic이 실시한 설문조사에 따르면 기업 중 20% 이상이 "admin", "12345"와 같은 비밀번호 기본값을 변경하지 않은 채 사용하는 것으로 나타났습니다.

또한, 많은 조직에서는 사람이 비밀번호를 만들도록 하고 있습니다. 이 때문에 자동화된 컴퓨터 툴로 사이버 범죄자가 쉽게 추측하거나 "크래킹" 할 수 있는 취약한 비밀번호가 만들어집니다. 이 문제를 더욱 악화시키는 것은 많은 사람들이 여러 계정에 똑 같은 비밀번호를 사용한다는 것입니다.

해킹으로 인해 일어나는 일 알아보기

특권 계정이 해킹을 당하면 공격자는 신뢰할 수 있는 직원이나 시스템 행세를 하며 침입자로 탐지되지 않고 악의적인 활동을 수행할 수 있습니다. 공격자는 침해에 성공한 후 일반적으로 침해된 특권 계정을 사용하여 IT 팀의 일상적인 업무 패턴을 염탐하고 학습합니다. 그 예로는 일상적인 일정, 시행 중인 보안 조치, 네트워크 트래픽의 흐름 등을 파악하는 일이 있습니다. 결국에는 공격자가 전체 네트워크와 운영 방식을 정확하게 이해할 수 있게 됩니다.

표적 네트워크에 대해 더 많은 것을 알게 되면 공격자는 정상적인 활동에 섞여 탐지를 피하고 네트워크 보안 경보가 발생하지 않도록 조심합니다. 공격자는 탐지를 피하는 방법을 파악한 다음 원격 액세스 툴을 설치하여 지속적인 액세스를 가능하게 합니다. 이 툴을 통해 공격자는 언제든지 원하는 때에 돌아와서 경보를 울리지 않고 악의적 활동을 수행할 수 있습니다.

공격자의 동기에 따라 공격자는 다음과 같은 목적으로 특권 계정을 사용할 수 있습니다.

- 시스템 기능을 손상시키거나 IT 관리자의 액세스를 비활성화합니다.
- 사기 또는 평판 훼손을 위해 민감한 데이터를 훔칩니다.
- 데이터를 손상시킵니다.
- 악성 코드를 주입합니다.
- 맬웨어를 설치합니다.

주목할 만한 사이버 보안 침해

중대한 보안 침해 사건의 영향이 궁금하십니까? 여기 몇 가지 **주목할 만한 예**가 있습니다.

- 2014년 초, 소수 직원의 로그인 자격 증명이 해킹되어 1억4,500만 개의 사용자 데이터 레코드가 유출되었습니다.
- 2015년, 미국 국토안보부의 직원 30,000명 이상에 대한 정보가 해킹되었습니다. 해커는 한 직원의 이메일 계정을 침해하여 데이터에 액세스할 수 있었다고 말했습니다.
- 널리 사용되는 클라우드 스토리지 회사인 Dropbox는 2012년에 해킹을 당한 사실이 2016년에야 밝혀졌습니다. 이 때문에 사용자 6,800만 명의 이메일 주소와 비밀번호가 인터넷에 유출되었습니다.

침해된 특권 계정은 정당한 사용자로 보이기 때문에 침해가 탐지되더라도 근본 원인을 찾거나 디지털 포렌식을 수행하기가 매우 어렵습니다.

경고

대부분의 조직이 시스템 침해에 대한 인시던트 대응 계획을 마련해 두었지만 침해된 특권 계정으로 인한 위험을 평가하지는 않았습니다. 3장에서는 특권 계정 침해와 악용을 방지하기 위해 취할 수 있는 조치를 설명합니다.

공격을 멈추려면 기존 IT 보안 이상의 대책이 필요

지금까지 대부분의 조직은 방화벽, 바이러스 차단 프로그램, 침입 탐지 솔루션 등 기존의 보안 경계 툴을 사용하여 정보를 보호해 왔습니다. 그러나, 빠르게 진화하는 클라우드, 모바일, 가상화 기술의 시대에는 중요한 자산 주위에 울타리나 방어용 구덩이를 구축해도 더 이상 효과가 없습니다.

디지털 업무 공간과 소셜 공간에서 사람들은 끊임없이 정보를 공유하며 비밀번호와 자격 증명을 알아내려는 사회 공학적 시도와 표적 스피어 피싱 공격(targeted spear phishing attack)에 노출되고 있습니다. ID를 도난당하면 공격자는 쉽게 탐지를 피해 기존 보안 경계를 우회하여 특권 계정을 악용할 수 있습니다.

특권 계정 자격 증명을 해킹당하면 단순한 경계 침해가 아니라 사이버 재앙을 초래할 수도 있습니다. 그러므로, "새로운 사이버 보안 경계"는 직원, 계약자 및 서드파티 파트너의 ID와 액세스 권한을 보호하는 데 집중해야 합니다.


팁

특권 계정 관리(PAM)을 활용하여 효과적인 정책과 베스트 프랙티스를 따르면 새로운 기술 채택을 가속하는 동시에 사이버 범죄의 다음 피해자가 되는 일을 방지할 수 있습니다. 3장에서는 특권 계정 비밀번호를 보호하는 방법과 비밀번호 침해를 방지하기 위해 할 수 있는 일에 대한 자세히 살펴봅니다.

이 장의 내용

- 시작할 때 답해야 하는 중요한 질문
- 포괄적인 PAM 보안 솔루션 개발
- PAM과 다른 보안 및 운영 기능의 통합

3장 특권 계정 관리 및 보호

이 장에서는 비즈니스 요구사항에 맞는 포괄적인 특권 계정 관리(PAM) 솔루션을 개발하는 데 도움이 되는 중요한 질문에 대한 답을 얻을 수 있도록 안내합니다. 특권 계정의 보안을 유지하고 이를 보호하기 위해 전체를 고려한 보안 접근법을 개발할 수 있도록 중요한 통합 고려 사항을 반드시 포함하십시오.

시작할 때 답해야 하는 중요한 질문

중요한 정보 자산을 보호하기 위한 모든 IT 보안 조치와 마찬가지로, 특권 계정을 관리하고 보호하려면 계획과 지속적인 프로그램이 필요합니다. 조직 내에서 어느 특권 계정에 우선 순위를 지정해야 하는지 파악하고 이러한 특권 계정을 사용하는 사람들이 허용된 사용 방식과 책임 사항을 분명히 알고 있는지 확인해야 합니다. PAM 보안 솔루션을 성공적으로 실행하기 전에, 계획 단계에서 다음의 몇 가지 질문에 먼저 답해야 합니다.

- **조직의 특권 계정을 어떻게 정의하시겠습니까?** 조직마다 다릅니다. 그러므로, 데이터, 시스템 및 액세스 권한에 의존하는 중요한 비즈니스 기능이 무엇인지 확인해야 합니다. 중요한 시스템을 분류해 놓은

재해 복구 계획을 재사용하면 유용할 수 있습니다. 먼저 복구해야 하는 중요한 시스템의 계정을 특권 계정으로 지정할 수 있습니다. 이 단계에서 특권 계정을 분류해 놓는 것이 좋은데, 그 이유는 여기서 분류를 해두면 비즈니스에 필요한 특권 계정을 확인하고 우선 순위를 지정할 수 있으며 이를 통해 나중에 보안 제어 조치를 적용할 때 더 쉽게 결정을 내릴 수 있기 때문입니다.


팁

특권 계정은 IT 운영에서 너무나 중요한 역할을 수행하므로 비즈니스 위험과 운영에 맞게 특권 계정을 지정해야 합니다. 누가 특권 계정에 대한 액세스 권한을 가질 수 있고 언제 이러한 계정을 사용할 수 있는지를 이해하면 보안 태세를 규정하는 데 도움이 됩니다.

고위험 계정이 사용될 때 이를 알고 있으면 IT 보안 매니저는 언제 어디서 민감한 정보가 노출될 수 있는지 알 수 있습니다. 특권 계정이 사용되는 방식을 파악하면 조직은 신속하게 보안 위험과 노출을 찾아내어 더 나은 결정을 내릴 수 있습니다.

- **누구에게 특권 계정에 대한 액세스가 필요합니까?** 특권 계정은 사람, 애플리케이션 및 서비스, 시스템, 인프라 계정으로 분류되어야 합니다. 이러한 분류를 통해 상호작용 및 각 특권 계정에 적용되는 보안 제어 조치의 수준을 결정할 수 있습니다. 예를 들어, 사람의 상호작용을 고려할 때 직원이 비밀번호를 알아야 하는지 또는 직원이 사용 전에 비밀번호를 확인해야 하는지 생각해 보십시오. 애플리케이션과 시스템의 경우, 얼마나 자주 비밀번호가 변경되도록 해야 하는지, 특권 계정을 사용할 수 있는 IP 주소를 제한할 수 있도록 해당 시스템까지의 경로가 정적(static)이어야 하는지 스스로에게 물어보십시오.
- **액세스가 필요한 서드파티 계약자를 이용합니까?** 특권 계정에 액세스가 필요한 서드파티 계약자는 가장 큰 위험요소 중 하나입니다. 그 이유는 계약자가 특권 계정에 액세스하고 이를 관리하는 방식을 완전히 통제할 수 없기 때문입니다. 최근 몇 년간 발생한 많은 침해 사건은 신용 카드, 집 주소, 직원의 건강 기록 등 개인 식별 정보와 같은 데이터가 들어 있는 계약자의 노트북이 도난당하거나 해킹당하여 발생했으며, 노트북에 있던 모든 데이터가 유출되었습니다. 이와 관련하여 매우 큰 대가를 치른 주요 데이터 침해 사고 중에는 2013년에 있었던 대형유통업체 Target의 데이터 유출 사고와 미 해군 데이터 유출 사고가 포함됩니다. 이 두 곳 모두 서드파티 계약자가 있었고 이 계약자가 침해를 당하면서 큰 피해로 이어진 것이었습니다.

- **특권 계정 사용을 위한 기간을 설정합니까?** 예를 들면, 회계 시스템의 경우 월말 또는 분기말에만 액세스가 필요할 수 있습니다. 백업 시스템은 일반적으로 예약된 시간에 실행됩니다. 무결성 검증 및 취약점 스캔은 예약된 침투 시간을 따를 것입니다. 특정 특권 계정이 사용되어야 할 시간을 알면 정상적 행동을 식별할 수 있고 이를 바탕으로 남용 또는 오용 가능성을 발견할 수 있습니다.

- **외부 공격자에 의해 특권 계정이 침해되면 어떤 일이 일어납니까?** 특권 계정이 침해될 경우에 대비하여 인시던트 대응 계획을 세워두셨습니까? 많은 조직들이 계정이 침해된 경우 이에 대응할 준비가 되어 있지 않으며 기본적으로 단순히 특권 계정의 비밀번호를 변경하거나 특권 계정을 비활성화하는 데 그칩니다. 그러나 이것만으로 충분하지 않습니다.

  
  기억할 사항

  특권 계정은 "왕국으로 가는 열쇠"입니다. 특권 계정이 외부 공격자에 의해 침해되면 해커는 맬웨어를 설치할 수 있으며 자신만의 특권 계정을 만들 수도 있습니다. 예를 들어, 도메인 관리자 계정이 침해된 경우라면 전체 액티브 디렉토리가 취약해졌다고 가정해야 합니다. 즉, 공격자가 쉽게 돌아오지 못하도록 전체 액티브 디렉토리를 복원해야 합니다.

- **내부자에 의해 특권 계정이 노출되거나 악용될 경우의 위험은 무엇입니까?** 내부자의 오용 또는 남용으로부터 특권 계정을 보호하려면 가장 중요한 시스템에 집중해야 합니다. 예를 들면, 대부분의 직원에게 동시에 프로덕션 시스템, 백업 시스템, 금융 시스템 등 모든 중요 시스템에 대한 액세스 권한을 주어서는 안 됩니다. 그리고, 조직 내에서 직무가 변경된 직원의 경우 이전 역할에서 사용한 액세스 권한을 그대로 두어서는 안 됩니다.

  
  기술적 정보

  2013년에 Edward Snowden이 미국 국가안보국(NSA)의 정부 기밀 정보를 공개적으로 노출한 사건은 내부자의 무단 액세스가 외부 해커의 공격만큼 치명적일 수 있음을 보여주는 주요 사례입니다.

- **특권 계정에 명시적으로 적용되는 IT 보안 정책이 있습니까?** 많은 기업의 경우 기업 IT 정책이 마련되어 있지만 적절한 특권 계정 사용 방식과 책임 사항에 대한 정책은 없는 경우가 많습니다. 특권 계정을 분명하게 정의하고 허용되는 사용 방식에 관한 정책을 세부적으로 규정하여 특권 계정을 별도로 취급하십시오. 특권 계정 사용에 관한 책임을 누가 져야 하는지에 대한 내용도 포함하십시오.

팁

- **정부 또는 업계 규정을 준수해야 합니까?** 기업이 규정을 준수해야 하는 경우 특권 계정의 보안을 유지하는 일이 필수적입니다. 많은 조직은 내부 정책 및 정부 또는 업계 규정을 준수하기 위해 정기 감사를 거쳐야 합니다. 이는 해커들이 신용 카드, 건강 기록, 금융 정보 등 민감한 정보에 액세스할 수 있으므로, 특권 계정이 감사를 받았고 보안이 유지되며 통제되고 있음을 증명해야 한다는 뜻입니다.
- **특권 계정 사용 및 노출에 대해 CISO에게 적극적으로 보고하고 있습니까?** 특권 계정에 무슨 일이 일어나고 있는지 적절히 관찰할 수 없다면 내부자 남용의 위험을 높이고 외부 공격자가 사용자 비밀번호를 얻은 후 권한을 승격할 위험을 높이게 됩니다. 침해가 발생할 경우, 특권 계정 사용 방식을 모니터링하면 디지털 포렌식 팀이 근본 원인을 파악하고 향후 사이버 보안 위협의 위험을 낮추기 위해 향상할 수 있는 중요한 제어 조치를 찾아내는 데 도움이 됩니다.

포괄적인 PAM 보안 솔루션 개발하기

PAM에 대한 여러 가지 질문(이전 섹션 참조)을 한 후에는(그리고 답까지 얻은 후에는) IT 환경을 가장 효과적으로 보호할 보안 조치를 실행할 수 있도록 준비를 더 잘 갖출 수 있습니다. 이 섹션에서는 포괄적인 PAM 보안 솔루션을 개발하기 위한 단계들을 안내합니다.

견고한 기반 위에 구축

특권 계정을 관리하고 보호하기 위한 견고한 기반을 구축하면 새로운 기술을 채택할 때 확장성과 유연성을 향상할 수 있습니다. 이러한 기반은 중요한 자산을 보호하고, 신뢰할 수 있으며 권한을 부여받은 직원만 적절한 데이터와 시스템에 액세스하도록 제한하는 데 핵심적으로 필요한 요소입니다.

팁

이러한 토대를 구축하는 데 중요한 두 가지 실천 사항은 다음과 같습니다.

- **특권 계정을 사용하고 이를 책임질 사람들에게 사이버 보안 인식 교육 제공:** 교육을 통해 특권 계정 보안의 중요성을 강조하고 조직에 해당되는 IT 보안 정책에 대해 설명해야 합니다. 임원들에 대한 교육도 실시하여 임원진의 동의와 지지를 얻으십시오.
- **특권 계정 검색, 보안 유지, 보호를 자동화하는 툴 찾기:** 모든 평가 대상 소프트웨어 툴은 특권 계정을 지속적으로 탐색하고, 특권 계정 비밀번호를 안전한 "금고"에 보관하며, 정기적으로 자동으로 비밀번호를 변경하고, 효과적으로 특권 계정의 활동을 모니터링하고 보고할 수 있는 기능을 갖추어야 합니다.

PAM 보안 규칙 및 제어 조치 마련

PAM 보안을 위해 중요한 단계 중 하나는 다음과 같이 규칙과 제어 조치를 설정하는 것입니다.

- **많은 내장형 특권 계정의 기본 ID와 비밀번호를 변경합니다.** 이 작업이 PAM 보안 향상을 위한 첫 번째 과제 중 하나가 되어야 합니다. 연구 결과에 따르면 다섯 개 조직 중 한 곳꼴로 "admin" 또는 "12345"와 같은 특권 계정 비밀번호 기본값을 변경하지 않은 것으로 나타났습니다. 이러한 기본값으로 설정된 자격 증명은 비밀번호를 크래킹하기가 너무나 쉽기 때문에 해커들이 가장 우선적으로 시도합니다.
- **책임 소재를 분명히 하기 위해 특권 계정에 대한 공식적인 비밀번호 정책을 작성합니다.** 정책은 해당 조직 고유의 특권 계정 카테고리 및 분류 결과를 기반으로 작성해야 합니다. 온라인으로 정책 템플릿을 찾을 수 있으므로 처음부터 새로 작성하지 않아도 됩니다.
- **특권 계정을 직접적으로 공유하지 마십시오.** 관리자들이 자격 증명을 공유하면 공격자는 매우 쉽게 권한을 승격하고 민감한 정보에 액세스할 수 있습니다. 특권 계정에 대한 액세스는 시간, 권한 범위, 요구되는 승인을 통해 제한해야 합니다. 예를 들면, 직원이 휴가를 가는 경우 해당 역할을 수행하기 위해 필요한 특권 계정을 다른 동료에게 할당 또는 위임할 수 있어야 합니다. 또한, 보안 제어 조치를 통해 이 동료가 특권 계정을 사용하여 얼마 동안 무엇을 할 수 있는지를 제한해야 합니다. 이는 경우에 따라서 이 동료가 특권 계정 비밀번호를 전혀 확인할 수 없을 수도 있음을 의미합니다.

- **민감한 데이터 또는 시스템을 사용하는 특권 계정 활동 세션을 모니터링하고 기록합니다.** 이렇게 하면 적절한 행동을 유도할 수 있고 직원과 다른 IT 사용자의 실수를 방지할 수 있습니다. 이들은 자신의 활동이 모니터링되고 있다는 것을 알고 있기 때문입니다. 또한, 세션을 기록하면 침해가 탐지되었을 때 침해의 원인을 밝혀내는 데 매우 귀중한 정보를 얻을 수 있습니다.
- **공식적인 검토 및 승인 프로세스를 통해 신규 특권 계정 생성 작업을 통제합니다.** 외부 공격자나 악의적인 내부자는 새로운 특권 계정을 생성하여 시스템에 포함시키려고 시도하는 경우가 많으므로 이 프로세스를 엄격하게 통제해야 합니다. 새로운 특권 계정을 생성하는 경우 동료 또는 매니저의 검토를 포함하는 구체적인 검토 및 승인 프로세스를 거쳐야 합니다. 또한, 자동화된 소프트웨어로 정기적인 탐색을 실행하여 새로운 특권 계정 또는 승인되지 않은 특권 계정을 찾아낼 수 있습니다.
- **특권 계정을 평가하여 적절한 만료일을 설정합니다.** 이 정책은 *특권 액세스 크립(privileged access creep)*이라고 알려진 현상을 예방할 수 있습니다. 특권 액세스 크립이란 사용자가 일정 기간 동안 지금은 필요하지 않을 수 있는 권한을 누적시키는 것을 말합니다. 특정 사용자에게 적합하지 않은 특권 계정, 특히 더 이상 액세스가 필요하지 않은 서드파티 계약자가 사용하는 계정을 검토하여 비활성화해야 합니다.
- **특권 계정을 "항시적"으로 사용하도록 허용하지 말고 "온디맨드" 방식으로 사용하도록 하십시오.** 특권 계정은 특정 작업 또는 목적을 위해서만 사용해야 합니다. 온디맨드 특권 계정 액세스를 지원할 경우 사용자는 직접 계정에 액세스하지 못하고 변경 관리 또는 제어 지점으로 가야합니다. 자동화된 PAM 소프트웨어를 사용하면 IT 관리자 직원은 의도된 목적을 위해서만 특권 계정을 사용할 수 있습니다.

  온디맨드 액세스는 일반적으로 계정 체크아웃, 승인 또는 최소 권한 모델이라고 부릅니다. 이 모델을 따르는 경우 관리자는 특권 계정을 사용할 때 업무상의 사유를 제시해야 합니다. 액세스가 허용된 경우에도 표준 계정 권한으로 제한해야 하며 명시된 작업이 필요한 경우에만 이 권한을 승격해야 합니다. 이렇게 하면 특권 계정 남용 또는 침해 위험을 크게 줄일 수 있습니다.

지속적으로 개선하기

이 섹션에서는 특권 계정 감사를 진행하고 규정 준수 사실을 증명하는 작업을 지속적으로 개선하기 위한 몇 가지 방법을 안내합니다.

특권 계정 활동 감사 및 분석

침해 또는 오용을 의미할 수 있는 비정상적인 행동을 발견하는 데 도움이 되는 감사와 보고서를 통해 특권 계정이 어떻게 사용되고 있는지 관찰하십시오. 또한, 이러한 자동화된 보고서를 통해 보안 인시던트의 원인을 추적하고 정책과 규정을 준수했음을 입증할 수 있습니다.

특권 계정을 감사하면 사이버 보안 지표를 얻을 수 있습니다. 이러한 사이버 보안 지표는 최고 정보 보안 책임자(Chief Information Security Officer, CISO)와 같은 임원들이 충분한 정보를 기반으로 비즈니스 결정을 내리는 데 필요한 데이터를 제공합니다. 감사와 분석을 함께 수행하면 특권 계정 침해 위험과 노출을 줄일 수 있는 강력한 툴이 될 수 있습니다.

규정 준수 사실 증명

강력한 규제가 시행되는 산업에서 일하거나 정부 지시를 충족해야 할 경우 필수적으로 규정 준수 사실을 증명할 수 있어야 합니다. PAM 보안은 이제 전반적인 사이버 보안 보호 전략에서 없어서는 안 될 구성요소로 간주됩니다.

지속적인 특권 계정 탐색

새로운 특권 계정이나 네트워크상의 계정 변경 사항을 지속적으로 찾아내려면 프로세스와 자동화된 툴이 필요합니다. 이는 중요한 정보 자산을 보호하는 데 필요한 가시성과 제어 능력을 유지하는 유일하고 실질적인 방법입니다.

PAM과 기존 보안 제어 조치의 통합

많은 사이버 보안 조치와 마찬가지로 PAM은 전략을 구성하는 중요한 요소 중 하나일 뿐입니다. 효과적으로 보안 전략을 실행하려면 PAM을 조직의 다른 보안 제어 조치와 통합하여 진화하는 위협으로부터 조직을 보호할 수 있는 보다 전체적인 사이버 보안 방패막을 제공해야 합니다.

PAM을 더 넓은 범위의 ID 및 액세스 관리(Identity Access Management, IAM)의 일부로 통합하면 모범 보안 관행에 따라 사용자 프로비저닝을 자동으로 제어하여 모든 사용자 ID를 보호할 수 있습니다. 또한, PAM 보안은 보안 정보 및 이벤트 관리(Security Information and Event Management, SIEM) 솔루션과도 통합되어야 합니다. 이렇게 하면 특권 계정과 관련된 보안 이벤트를 보다 전체적으로 이해할 수 있고 IT 보안 직원에게는 시정 조치나 추가적인 분석이 필요한 보안 문제를 더 효과적으로 알려줄 수 있습니다.

기억할 사항

또한, PAM을 사용하여 취약성 평가, IT 네트워크 인벤토리 스캔, 가상 환경 보안, ID 거버넌스, 관리 및 행동 분석에 대한 인사이트를 개선할 수 있습니다. 특권 계정 보안에 특별한 관심을 기울이면 모든 사이버 보안 노력을 향상하여 조직을 가장 효율적이고 효과적인 방식으로 보호할 수 있습니다.

PAM 보안을 위한 포괄적인 계획을 실행하면 사이버 위협으로부터 조직을 보호할 수 있습니다. Thycotic이 실시한 해커에 대한 조사에 따르면, 특권 계정에 대한 액세스를 제한하면 해커가 활동하기가 더욱 어려워지고 조직의 보안은 더욱 강화되는 것으로 나타났습니다.

PAM 다음에는 무엇이 올까요?

앞으로 몇 년에 걸쳐 PAM 및 IAM이라는 IT 카테고리는 합쳐질 가능성이 높습니다. 이는 사용자의 디지털 ID가 한곳의 고용주뿐만 아니라 여러 산업과 정부 기관에서 사용될 것임을 의미합니다. 투표, 은행 업무, 여행, 문 열기, 자동차 시동 걸기, 대중 교통 이용, 의료 서비스 이용 등에 편리하게 사용할 수 있는 디지털 ID를 상상해 보십시오. IAM 분야에서 블록체인 기술이 등장하고 있으며 이 기술은 사용자가 서비스형 클라우드에서 제공되는 모든 것에 액세스할 수 있도록 부인 방지(nonrepudiation) 기능 및 무결성을 제공합니다.

또한, PAM은 직원, 타사, 다수의 애플리케이션, 네트워크 시스템에 대한 신뢰 수준을 결정하는 행동 분석 기능도 추가하고 있습니다. 이러한 기능은 가까운 미래에 ID 및 신뢰 검증 역량을 새로운 차원으로 끌어올려 사이버 보안 관리를 더욱 신뢰할 수 있는 방식으로 수행하도록 지원할 것입니다.

이 장의 내용

» 해커의 활동을 더 어렵게 만들기

» PAM 솔루션 실행을 도와줄 파트너 선택하기

4장 조직을 보호하는 주요 방법

특권 계정 관리(PAM)는 극복할 수 없는 과제가 아닙니다. 어느 조직이든 아래의 실용적인 팁을 따르면 특권 계정을 관리 및 보호하고 보안을 유지할 수 있습니다(그리고 해커의 활동을 더 어렵게 만들 수 있습니다.)

» **PAM을 위한 수작업 관행 피하기:** 특권 계정의 비밀번호를 추적하고 직원들 사이에서 이를 공유하기 위해 아직도 Microsoft Excel 스프레드시트에 의존하는 조직이 너무 많습니다. 이와 같은 수작업 관행은 위험하고 비효율적입니다. 자동화된 PAM 소프트웨어 솔루션은 간편하게 설치가 가능하고 최소의 노력으로 관리할 수 있습니다. 이러한 솔루션으로 시간과 비용을 절약하고 해커와 악의적인 내부자로부터 조직에 대한 보호를 크게 강화할 수 있습니다.

» **직원 교육 실시:** 대부분의 조직에서 보안을 가장 취약하게 만드는 요인은 사람입니다. 더욱 정교한 사회 공학 및 피싱 공격이 등장함에 따라, 조직은 단순한 온라인 테스트나 보안 정책에 대한 교육 이상의 IT 보안 인식 프로그램을 마련해야 합니다. 비즈니스 목적의 개인용 모바일 디바이스가 점점 더 많이 사용되고 있으므로 직원들에게 안전한 사용 방법을 반드시 교육해야 합니다.

- **특권 계정 및 SSH(Secure Shell) 키 관리를 위한 탐색과 자동화:** 전용 PAM 소프트웨어 솔루션을 사용하고, 먼저 가장 중요하고 민감한 특권 계정에 집중하고, 특권 계정의 무분별한 증가를 억제하기 위해 지속적으로 탐색하고, 내부자의 남용 가능성을 파악하고, 외부적 위협을 찾아내십시오. 이렇게 하면 사이버 보안 위협에 대처하는 데 필요한 특권 계정 환경에 대한 가시성을 지속적으로 확보할 수 있습니다.
- **IT 관리자의 시스템 액세스 제한:** *최소 권한 전략*에 따라 액세스를 제한하십시오. 즉, 권한이 필요하고 이에 대한 승인을 받은 경우에만 권한을 부여하십시오. 최종 사용자를 표준 사용자 프로필로 구성하고 승인된 애플리케이션을 실행할 경우에만 권한을 자동으로 승격하여 최종 사용자 워크스테이션에 최소 권한을 부여하십시오. IT 관리자인 사용자의 경우 액세스를 통제하고 Windows 및 UNIX 시스템에 대해 슈퍼 유저 권한 관리를 실행하여 공격자가 악성 애플리케이션, 원격 액세스 툴, 명령을 실행하지 못하도록 해야 합니다.
- **특권 계정 비밀번호 보호:** 비밀번호 보호 소프트웨어를 사용하여 특권 계정 액세스를 사전에 관리, 모니터링, 통제하십시오. 이 솔루션은 자동으로 특권 계정을 탐색 및 보관하고, 비밀번호 변경을 예약하고, 개별 특권 계정 세션 활동을 감사, 분석, 관리하고, 비밀번호 계정을 모니터링하여 악의적 활동을 신속하게 탐지하고 이에 대응할 것입니다.
- **특권 애플리케이션 및 알려지지 않은 애플리케이션 제한:** 애플리케이션 계정의 목록을 작성하고 비밀번호의 강도, 계정 액세스 및 비밀번호 변경과 관련하여 엄격하게 정책을 적용해야 합니다. 최소 권한을 적용하고 애플리케이션 관리 솔루션을 활용하면, 승인되지 않은 애플리케이션을 실행할 위험을 최소화하면서 승인되고 신뢰할 수 있는 화이트리스트로 지정된 애플리케이션을 원활하게 승격할 수 있습니다.
- **PAM 솔루션 파트너 선택:** 시스템과 민감한 데이터에 대한 액세스를 통제하고 정책과 규정을 준수하여 궁극적으로 회사를 더 안전하게 보호하도록 지원하는 신뢰할 수 있는 파트너와 종합적인 PAM 솔루션을 실행하십시오.

팁

ID 확인을 자동화할 수 있는 소프트웨어 솔루션을 찾고 스토리지를 지속적으로 모니터링 및 기록하고 보안을 적용하면서 특권 계정에 대한 위험을 파악하십시오.

지금 보안 환경을 개선하십시오!

Thycotic이 제공하는 무료 특권 계정 관리 툴박스

침해를 방지하고 "왕국으로 가는 열쇠"를 보호하기 위한 혁신적인 학습 툴과 자동화된 무료 툴

무료

학습 툴

무료 특권 계정 비밀번호 보안 온라인 교육(Privileged Password Security Online Training)을 통해 여러분과 직원은 특권 계정 보안의 중요성과 비밀번호 보호를 위한 모범 지침에 대한 최신 정보를 얻을 수 있습니다.

특권 계정 비밀번호용 무료 보안 정책 템플릿(Free Security Policy Template for Privileged Passwords)은 보안을 향상하고 규정 준수 의무를 수행하도록 지원하는 맞춤 구성하기 쉬운 템플릿을 제공하므로 시간과 노력을 절약할 수 있습니다.

무료

보안 툴

Windows용 무료 취약 비밀번호 탐색기(Weak Password Finder for Windows)가 조직 내 어디에서 취약한 비밀번호가 사용되는지 찾아낼 수 있는 쉽고 빠른 방법을 제공합니다.

Windows용 무료 특권 계정 탐색 툴(Privileged Account Discovery for Windows)을 통해 기업의 특권 계정을 찾을 수 있습니다. 이 중에는 알려지지 않았거나 관리되지 않는 특권 계정도 포함됩니다.

Windows용 무료 엔드포인트 애플리케이션 검색 툴(Windows Endpoint Application Discovery)을 통해 취약한 애플리케이션과 이와 관련된 위험을 몇 분 안에 찾아낼 수 있습니다.

무료

벤치마크 툴

무료 비밀번호 취약성 벤치마크(Password Vulnerability Benchmark)를 통해 동료에 비해 여러분의 비밀번호 보호 노력이 얼마나 효과적인지 알아볼 수 있습니다.

무료 보안 측정 인덱스 온라인 설문조사가 여러분의 IT 보안 노력이 모범 지침과 동료의 보안 노력에 비해 얼마나 효과적인지 알려줍니다.

지금 다운로드: thycotic.com/free-tools

thycotic

보안 위협으로부터 조직을 보호하십시오.

외부 공격자와 악의적인 내부자가 제기하는 정교하고 집중된 보안 위협 때문에 조직이 중요하고 민감한 정보를 적절하게 보호하는 일이 매우 어려워졌습니다. IT 환경이 더욱 복잡해지고 널리 분산되면서 이러한 자산을 보호하는 일도 더 어려워졌습니다. *초보자를 위한 특권 계정 관리*, Thycotic 스페셜 에디션은 IT 네트워크와 특권 계정 및 비밀번호 사용 시 노출을 관리하는 데 도움이 됩니다.

주요 내용...

- 특권 계정과 사용자 계정의 유형
- 비밀번호 관리 및 보호
- 사이버 범죄자 억제
- 침해된 계정이 제기하는 위험
- PAM과 보안 기능의 통합
- PAM 파트너 선택

thycotic

Joseph Carson은 엔드포인트 보안, 애플리케이션 보안, PAM을 전문으로 하여 엔터프라이즈 보안 분야에서 25년 넘게 경력을 쌓은 사이버 보안 전문가입니다. Joseph는 CISSP이며 사이버 커뮤니티에서 활동 중인 회원으로, 전 세계적으로 개최되는 사이버 보안 컨퍼런스에서 발표자로 활동 중입니다. 그는 여러 정부뿐만 아니라 중요 인프라, 금융 및 해양 산업을 위한 사이버 보안 자문으로도 일하고 있습니다.

Dummies.com®에서
비디오, 단계별 사진, 방법 안내 문서를
확인하고 쇼핑도 해보십시오!

for dummies®
A Wiley Brand

ISBN: 978-1-119-38684-1
증정용