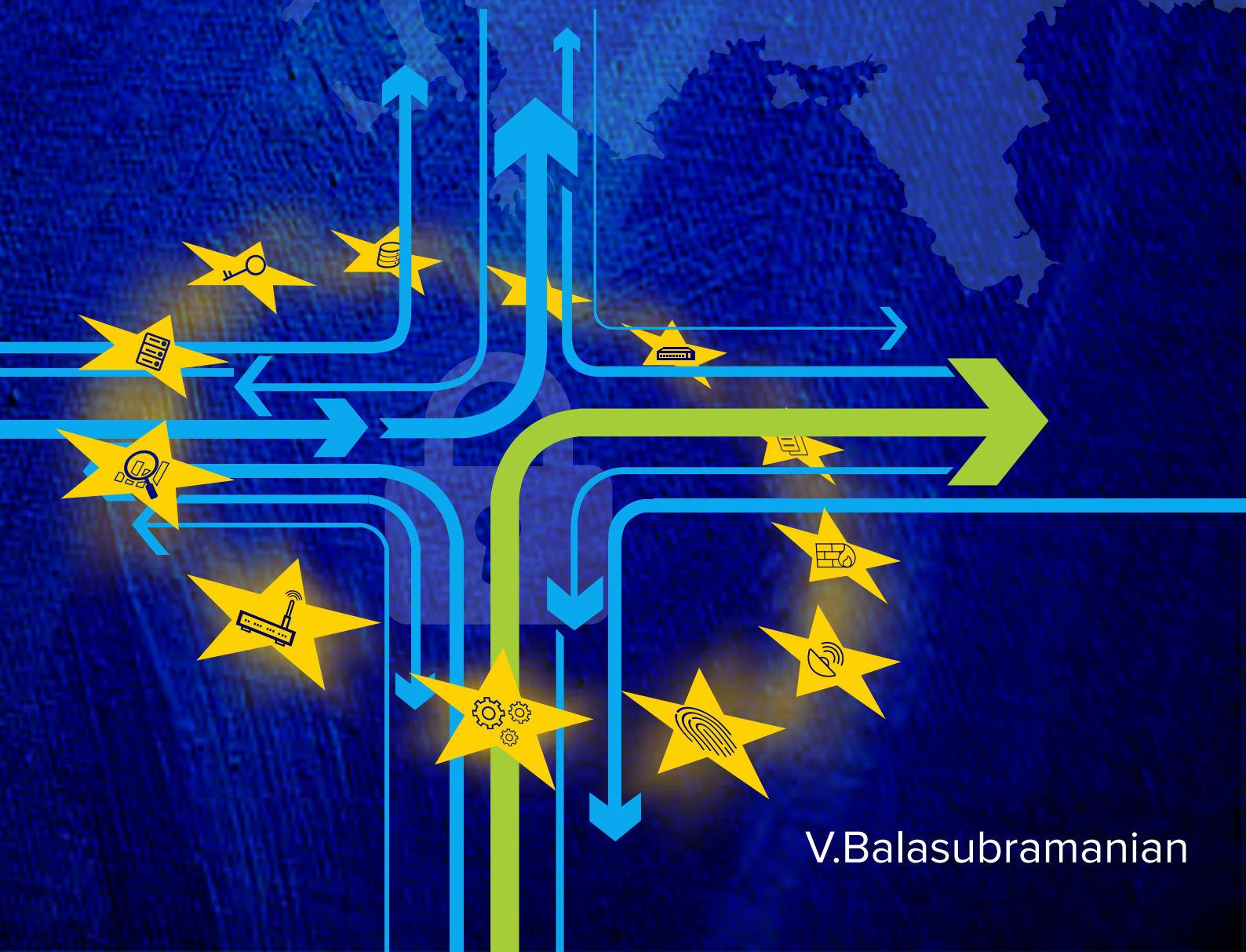
ManageEngine
Password Manager Pro

Lösungen für den Umgang mit der EU-DSGVO

DSGVO Compliance:
Das privilegierte Zugangsmanagement ist (nur) der erste Schritt



V.Balasubramanian

Was ist das Hauptziel der DSGVO?

Der Countdown zum Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) der EU hat begonnen – und Unternehmen bleibt nicht mehr viel Zeit. Während in den Medien viel Aufhebens gemacht wird und Anleitungen sowie Lösungen verbreitet werden, sind abschließende Interpretationen zur DSGVO und ihren verschiedenen Aspekten jedoch noch gar nicht erfolgt. Das grundlegende Ziel der DSGVO ist jedoch überdeutlich: mehr Datenschutz, bzw. genauer gesagt mehr Schutz für personenbezogene Daten.

Der Begriff *„personenbezogene Daten“* nimmt in der DSGVO einen breiten Raum ein. Darunter fallen alle Informationen, die sich auf eine *„identifizierbare natürliche Person“* beziehen. Unternehmen und andere Organisationen verarbeiten und speichern üblicherweise Kundennamen, E-Mail-Adressen, Fotografien, Arbeitsinformationen, Konversationen, Mediendateien und weitere Informationen, mit deren Hilfe sich Individuen identifizieren lassen.

Personenbezogene Daten sind omnipräsent und demnach auch fast überall in der IT. Wenn sich Ihr Unternehmen an die Vorschriften der DSGVO halten will, müssen Sie strikte Zugangskontrollen festlegen und durchsetzen. Außerdem müssen Sie genau nachweisen, wer auf welche Weise Zugriff auf Informationen erhält.

Privilegierter Zugang und Gefahren für die Datensicherheit

Cyber-Attacken können sowohl innerhalb eines Unternehmens als auch außerhalb ihren Ursprung haben. Analysen prominenter Angriffe aus der letzten Zeit zeigen, dass interne wie externe Angreifer privilegierte Zugänge nutzen, um ihre Attacken durchzuführen. Meist sind dabei personenbezogene Daten das Ziel, wie sie IT-Anwendungen und -Geräte verarbeiten und speichern. Sicherheitsexperten weisen immer wieder darauf hin, dass heutzutage nahezu alle Arten von Cyber-Attacken privilegierte Konten einbeziehen.

Privilegierte Konten sind das Hauptziel von Cyber-Kriminellen

Der unberechtigte Zugang zu privilegierten Konten sowie deren Missbrauch ist der *„Schlüssel zum Reich der IT“* – Cyber-Kriminelle nutzen ihn sowohl bei internen wie externen Attacken als vorrangige Methode. Dabei zielen sie bevorzugt auf Administrator-Kennwörter, System-Default-Konten sowie fest kodierte Berechtigungsdaten in Skripten und Anwendungen, um sich Zugang zu verschaffen.

Typischerweise setzen Hacker sogenannte Phishing- oder Spear-Phishing-Methoden ein, um sich des Computers eines Endanwenders zu bemächtigen. Gelingt ihnen das, installieren sie Malware und suchen nach den Administrator-Passwörtern. Mit ihnen erhalten die Angreifer uneingeschränkte Zugangsprivilegien zu allen Bereichen des Netzwerks. So können sie alle Computer infizieren und Daten abgreifen. In dem Moment, in dem der Hacker Zugang zu einem Administrator-Passwort erlangt, wird die gesamte Organisation verwundbar für Attacken und Datendiebstahl. Perimeter-basierte Sicherheitsmaßnahmen können nicht vollständig gegen diese Art von Attacken schützen.

Gefahr von innen und außen

Jede Organisation muss mit Dritten zusammenarbeiten: Lieferanten, Geschäftspartner, Subunternehmer etc. – nur mit Partnern lässt sich die Vielzahl unternehmerischer Aufgaben erledigen. Oftmals erhalten Außenstehende daher einen privilegierten Remote-Zugang zu physischen und virtuellen Ressourcen innerhalb eines Unternehmens oder einer Organisation.

Auch wenn Sie selbst robuste Sicherheitsvorkehrungen getroffen haben, wissen Sie nicht, wie Dritte mit Ihren Daten umgehen. Hacker könnten einfach Schwachstellen Ihrer Partner ausnutzen oder Phishing-Attacken gegen jene richten, die Zugang zu Ihrem Netzwerk haben. Deshalb ist es unbedingt erforderlich den privilegierten Zugang von außen zu regulieren, zu verwalten und zu überwachen.

Leider zählen Personen innerhalb Ihres Unternehmens ebenfalls zu den potenziellen Gefahrenquellen. Verärgertes IT-Personal, unbedachte oder entlassene Mitarbeiter – es hat in der Vergangenheit zu viele Fälle von Angriffen aus dem Inneren gegeben, als dass IT-Abteilungen sie vernachlässigen könnten.

Zu leicht lassen sich ohne entsprechende Vorkehrungen zum Beispiel Logikbomben platzieren oder Daten stehlen. Nicht regulierte Administrator-Zugänge sind daher eine Sicherheitsbedrohung, die ganze Unternehmen in Gefahr bringen können.

Der erste Schritt zur Beachtung der DSGVO-Richtlinie: Management der privilegierten Zugänge

Regulieren, überwachen und verwalten Sie den privilegierten Zugang zu Ihrem Unternehmen

Die DSGVO verlangt, dass Unternehmen die Richtlinien zum Schutz personenbezogener Daten einhalten. Das wiederum erfordert die vollständige Kontrolle über privilegierte Zugänge. Um das zu erreichen, müssen Sie…

- ☑ alle privilegierten Konten konsolidieren und sie in ein sicheres, zentrales Depot überführen
- ☑ starke, einzigartige Passwörter vergeben und deren regelmäßige Aktualisierung durchsetzen
- ☑ den Zugriff auf Konten auf Basis von Rollen und Verantwortlichkeiten einschränken
- ☑ für den Abruf von Passwörtern besonders sensibler Bereiche zusätzliche Vorkehrungen treffen

- ☑ den Zugang zu privilegierten Konten auditieren
- ☑ fest kodierte Berechtigungen in Scripts und Anwendungen komplett eliminieren
- ☑ wo immer möglich den Fernzugang zu IT-Systemen nur gewähren, ohne die Berechtigungen in Klartextform zu übermitteln
- ☑ strikte Zugangskontrollen für Dritte durchsetzen und die Aktivitäten Außenstehender in der eigenen IT genau verfolgen
- ☑ doppelte Kontrollen einrichten, um Sessions zu überwachen, die über einen privilegierten Zugang zu hochsensiblen IT-Assets erfolgen
- ☑ privilegierte Sitzungen für forensische Audits aufzeichnen

Angemessene Regulierung, Überwachung und Verwaltung erfordern die Automatisierung des gesamten Lebenszyklus privilegierter Zugänge. Manuelles privilegiertes Zugangsmanagement wäre zeitaufwändig, fehleranfällig und könnte mit hoher Wahrscheinlichkeit nicht den gewünschten Sicherheitsstandard gewährleisten.

Privilegiertes Zugangsmanagement mit dem Password Manager Pro von ManageEngine automatisieren – und so für DSGVO bereit sein

Password Manager Pro ist eine umfassende webbasierte Softwarelösung zur Verwaltung sensibler Informationen wie Passwörter, Dokumente oder digitale Identitäten. Die Password-Management-Software ist das perfekte Tool für Unternehmen, die Konten mit weitgehenden Zugriffsrechten, etwa von Superusern und Administratoren, überwachen und zuverlässig vor Missbrauch schützen wollen – von der Regulierung, Verwaltung und Überwachung bis hin zum Auditing des gesamten Lebenszyklus privilegierter Zugänge. Password Manager Pro bietet drei Lösungen in einem Paket: Privileged Account Management, die Verwaltung von Remote-Zugängen sowie das Management von privilegierten Sitzungen.

Die Software verschlüsselt und konsolidiert alle Ihre privilegierten Konten in einem zentralen Depot, das durch granulare Zugangskontrollen zusätzlich geschützt ist. Password Manager Pro entschärft IT-Security-Risiken im Zusammenhang mit privilegierten Zugängen und verhindert so Sicherheitsverletzungen und Compliance-Probleme, bevor diese Ihr Unternehmen lahmlegen können.

Diese Funktionen geben Ihnen die komplette Kontrolle über privilegierte Zugänge und legen damit ein solides Fundament für die Compliance mit der DSGVO.

Password Manager Pro: Lösungen

1. Management privilegierter Konten

Password Manager Pro schützt Ihre privilegierten Konten, indem es bewährte Passwort-Management-Praktiken durchsetzt. Dazu zählen etwa eine zentrale Passwortspeicherung, die Vergabe von starken Passwörtern, das regelmäßige Zurücksetzen von Passwörtern sowie Zugriffskontrollen für gemeinsame Passwörter in Ihrem Unternehmen.

Automatische Erkennung von Geräten

Automatisieren Sie die Erkennung der IT-Assets in Ihrem Netzwerk, und listen Sie privilegierte Konten auf.

Periodische Änderung der Passwörter

Accounts erhalten automatisch neue Passwörter, um mögliche Schwachstellen zu beseitigen.

Konsolidieren und Speichern

Erfassen Sie alle privilegierten Identitäten in einem zentralen Depot, das mit einer AES-256-Verschlüsselung gesichert ist.

Organisieren und Aufräumen

Organisieren Sie Ihre Ressourcen in Gruppen und vereinfachen Sie so deren Management.

Passwort-Regeln

Setzen Sie Regeln durch, die beispielsweise die Komplexität der Passwörter und das Ablaufdatum bei periodischer Passwortänderung festlegen.

Sicheres Teilen

Teilen Sie mit Ihren Team-Mitgliedern nach Bedarf Administrator-Passwörter mit granularen Zugangsbeschränkungen.

Workflow bei Zugangskontrollen

Benutzer müssen sich einem „Request-Release"-Mechanismus unterziehen, bevor sie Zugriff auf Passwörter erhalten. Dieser ist zeitlich begrenzt, folgt dem Least-Privilege-Prinzip (Nutzer, Anwendungen, Dienste etc. erhalten nur diejenigen Rechte, die zur Erfüllung der jeweiligen Aufgaben unbedingt notwendig sind) und unterliegt zweifachen Kontrollen.

Remote-Passwort-Zurücksetzung

Passwörter für Remote-Ressourcen können sofort nach Gebrauch automatisch zurückgesetzt werden.

Regelmäßige Überprüfung der Passwort-Integrität

Password Manager Pro kann automatisch regelmäßige Integritätsprüfungen von Passwörtern durchführen. So können Sie erkennen, ob die gespeicherten Passwörter mit Remote-Ressourcen übereinstimmen.

Windows Service Account Management

Setzen Sie Passwörter für Windows Domain-Konten zurück. Neue Passwörter werden automatisch an alle abhängigen Services und Anwendungspools übermittelt.

Post-reset Scripts

Lassen Sie automatisiert weitere Maßnahmen nach der Remote-Passwort-Zurücksetzung durchführen, wie etwa den Neustart von Services.

Application-to-Application (A-to-A) Password Management

Lassen Sie Password Manager Pro die Passwörter für Ihre Anwendungen geschützt über die API abrufen, und eliminieren Sie so auch fest codierte Berechtigungen.

FIPS 140-2 Compliant-Modus

Erfüllen Sie Compliance-Vorgaben mit nach FIPS 140-2-validierten kryptografischen Modulen.

Unterbrechungsfreier Zugriff

Mit der Hochverfügbarkeits-Einstellung gewährleistet Password Manager Pro lückenlosen Zugriff auf kritische Passwörter und bietet Backup-Möglichkeiten.

Mobilität

Greifen Sie mit nativen Apps für iOS, Android und Windows von überall aus auf Passwörter zu.

2. Management von Remote-Zugängen

Password Manager Pro verschafft Ihnen mit nur einem Klick sicheren Zugriff auf alle Remote-Geräte, die zunächst eine Verbindung zu Jump Servern benötigen, um dann zu den Zielgeräten zu „springen" – das gilt auch für Remote-Rechenzentren. Password Manager Pro zentralisiert die Verwaltung all dieser Berechtigungen und Zugangskontrollen, so dass sich Benutzer nicht auf jeder Stufe des Remote-Zugangs neu authentifizieren müssen. Alle Login- und Authentifizierungsschritte werden automatisch vorgenommen.

Erstklassiger Fernzugang

Starten Sie eine hochsichere, zuverlässige und komplett emulierte Windows RDP-, SSH-, Telnet- oder SQL-Sitzung – ein Klick über jeden HTML5-kompatiblen Browser genügt, ohne zusätzliche Plug-Ins oder Agent-Software.

One-Click-Login ohne sichtbare Passwörter

Mit den sicheren Gateways von Password Manager Pro können Sie Mitarbeitern und Dritten Fernzugriff gewähren, ohne die Passwörter im Klartext weiterzugeben.

Jump-Server-Konfiguration

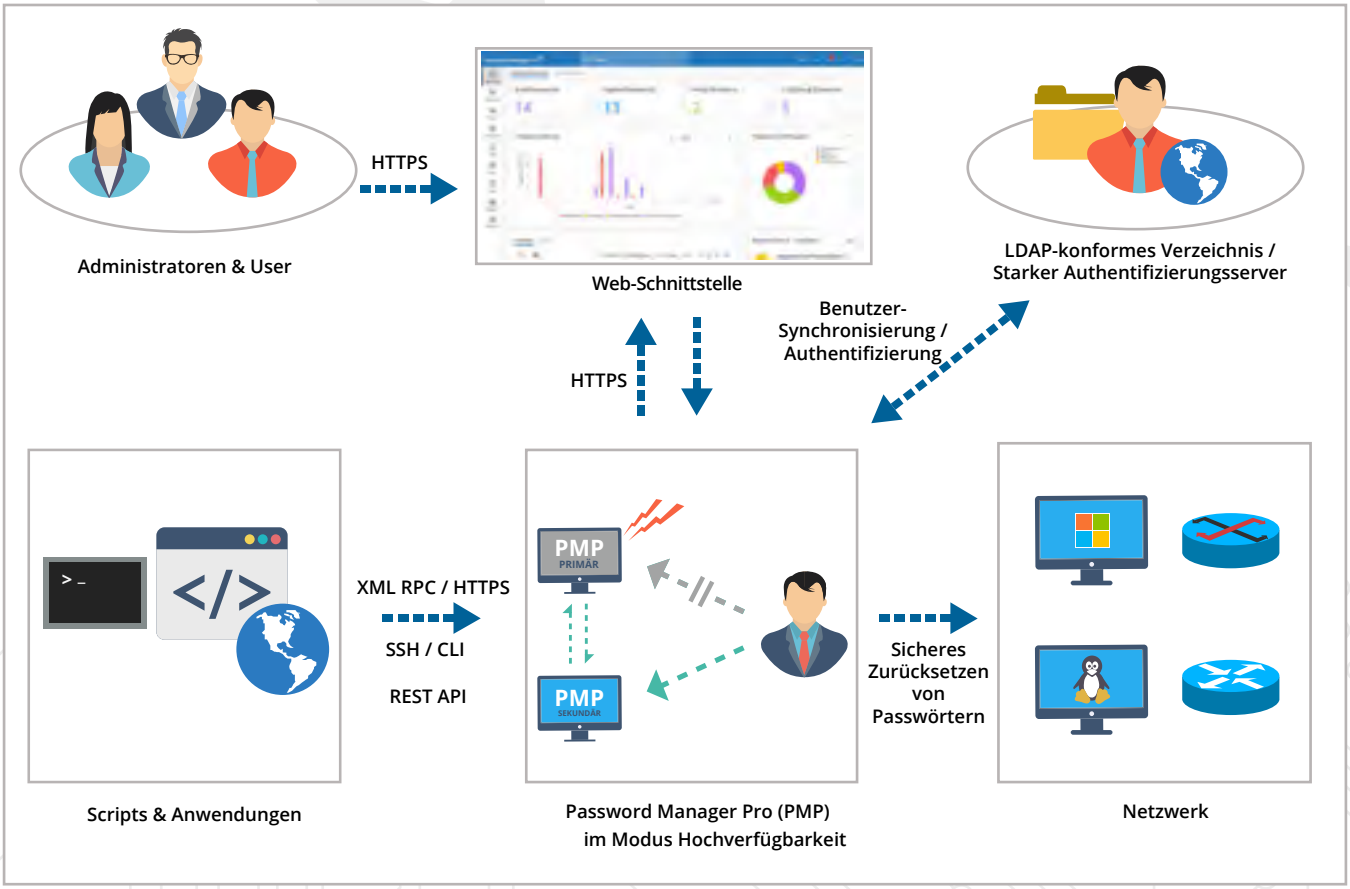
Vernetzen Sie sich direkt mit Ressourcen in Remote-Rechenzentren, ohne über verschiedene Zwischenstationen navigieren zu müssen.

Automatischer Login für Websites und Anwendungen

Starten Sie mit den nativen Erweiterungen von Password Manager Pro für Chrome und Firefox automatische Verbindungen zu Websites.

Sichere Datenübertragung

Sichere Kommunikationsprotokolle (HTTPS und SSL) gewährleisten die Datenintegrität während der Übertragung.

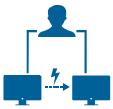


3. Management privilegierter Sitzungen

Mit Password Manager Pro können Sie privilegierte Sitzungen bedarfsgerecht überwachen und steuern. So lässt sich lückenlos nachverfolgen, ob User den privilegierten Zugang gemäß der Unternehmensrichtlinien nutzen.

Mitschnitt von Sitzungen

Password Manager Pro zeichnet privilegierte Sitzungen per Video auf und archiviert diese, damit sie für forensische Audits herangezogen werden können.



Doppelte Kontrollen

Überwachen Sie privilegierte Sitzungen in Echtzeit, um bei verdächtigen oder schädigenden Aktivitäten den Zugang des jeweiligen Users sofort beenden zu können.

Vollständige Audit-Aufzeichnungen

Greifen Sie jederzeit auf archivierte Aufzeichnungen zurück, um festzustellen, wer wann welchen privilegierten Zugang erhalten hat.

Compliance-Berichte

Mit integrierten Berichtsvorlagen können Sie Compliance-Berichte nach ISO/IEC 27001 und NERC-CIP erstellen lassen, um die Vorgaben für die Nutzung privilegierter Kennungen zu dokumentieren.

Die von Password Manager Pro entschärften IT-Sicherheitsrisiken

Produktfunktionen vs. entschärfte Risiken

Management privilegierter Konten

Account-Erkennung, Passwortschutz & -verwaltung

Password Manager Pro erkennt automatisch die IT-Assets im Netzwerk (Windows, Linux, Netzwerkgeräte sowie virtuelle Maschinen) und listet die mit ihnen verbundenen, privilegierten Konten auf. So können Unternehmen schnell alle privilegierten Identitäten schützen.

Folgende Risiken entschärft dieser Erkennungsprozess:

Identifizieren Sie unautorisierte Konten oder Services:

Password Manager Pro listet alle privilegierten Konten auf, die Ihren kritischen IT-Assets zugeordnet sind. Anhand eines internen Audits können Sie unautorisierte Konten einfach identifizieren.

Reduzieren Sie die Anzahl privilegierter Konten:

Der Erkennungsprozess macht auch nicht mehr benötigte Konten ausfindig. Sie können dabei festlegen, welche absolut notwendige Konten erhalten bleiben sollen.

> Password Manager Pro von ManageEngine ist einfach zu nutzen und mühelos bereitzustellen. Administratoren können damit alle Zugriffe über ein einziges Interface überwachen und auditieren. Gleichzeitig bietet die Lösung großartige Funktionen zu einem überzeugenden Preis-Leistungs-Verhältnis.
>
> ★★★★★
>
> **SC** MAGAZINE
> Produktgruppen-Test
> (Privilegiertes Zugangsmanagement)

Verhindern Sie unberechtigten Zugang:

Indem Sie nach der Identifizierung privilegierter Konten neue Passwörter willkürlich vergeben, können Sie den unberechtigten Zugriff durch aktuelle oder ehemalige IT-Mitarbeiter verhindern.

Zentrales Passwort-Repository

Password Manager Pro konsolidiert, speichert und organisiert all Ihre Passwörter in einem geschützten, zentralen Repository. Das kann Sie vor folgenden Risiken schützen:

Vermeiden Sie, dass Passwörter aufgrund unsicherer Speicherung in falsche Hände geraten:

Netzwerk- und IT-Administratoren speichern häufig sensible Anmeldeinformationen in Textdateien und Kalkulationstabellen – und halten sie bisweilen sogar als Haftnotizen auf Papier fest. Solche riskanten Speicherpraktiken verwandeln Unternehmen in wahre Hacker-Paradiese. Password Manager Pro eliminiert derartige Schwachstellen durch das geschützte, zentrale Passwort-Repository.

Keine Systemsperrungen durch nicht aktuelle Passwörter:

Zirkulieren im Unternehmen inkonsistente Kopien elektronischer Dateien mit sensiblen Passwörtern, können diese veralten – so entstehen leicht Koordinierungsprobleme, die sich negativ auf die operative Effizienz auswirken. Mit seinem zentralen Repository vermeidet Password Manager Pro derartige Herausforderungen und Systemsperrungen.

Zugangsbereitstellung und -steuerung

Eigentümerschaft und granulares Teilen von Passwörtern

Die grundlegende Struktur von Password Manager Pro richtet sich nach dem Konzept der Eigentümerschaft sowie des Teilens von Passwörtern: Fügt ein Benutzer dem Repository ein Passwort hinzu, wird er automatisch Eigentümer dieses Passworts und erhält alleinigen Zugriff. Möchte er es für andere sichtbar machen, muss er es teilen. Alle Benutzer – IT-Administratoren eingeschlossen – können nur die Passwörter sehen, deren Eigentümer sie sind und diejenigen, die geteilt wurden.

Ungenutzte Konten deaktivieren:

Ungenutzte Accounts sind aktive privilegierte, aber inhaberlose Konten. Sie treten vor allem auf, wenn Mitarbeiter die Abteilung oder das Unternehmen wechseln; das gilt auch für IT-Administratoren. Werden diese Accounts nicht deaktiviert oder auf einen anderen Inhaber übertragen, können Lücken in der Zugangskontrolle entstehen. Password Manager Pro löst dieses Problem, indem ausscheidende Kollegen (reguläre und IT-Administratoren) die Eigentümerschaft an ihren Ressourcen auf einen anderen autorisierten Mitarbeiter transferieren können.

Die Weitergabe von Passwörtern durch unsicheres Teilen verhindern:

Häufig teilen sich (IT-)Mitarbeiter geläufige Passwörter innerhalb des Teams mündlich, per E-Mail oder Anruf mit – ein solches Vorgehen gefährdet natürlich die Sicherheit des Passworts. Password Manager Pro bietet eine integrierte rollenbasierte Funktion für sicheres, granulares Teilen. Das hilft, Passwörter geheim zu halten.

Keine unnötigen Zugriffe:

Password Manager Pro führt strenge Zugriffskontrollen durch. So ist sichergestellt, dass Administratoren ausschließlich die Passwörter im Repository einsehen können, die sie auch für ihre Rolle benötigen. Beispielsweise erhalten Windows-Administratoren keinen Zugriff auf Datenbank-Passwörter. So können Unternehmen verhindern, dass nicht involvierte Mitarbeiter in geschützten (IT-)Bereichen aktiv werden.

Keine Anzeige von Passwörtern im Klartext:

Auch wenn Passwörter auf dem sichersten Weg geteilt werden, lassen sie sich immer noch speichern oder notieren – und können so in falsche Hände gelangen. Als zusätzliches Sicherheitsfeature versetzt Password Manager Pro Administratoren in die Lage, Benutzern bei Bedarf Zugriff auf IT-Ressourcen zu erteilen, ohne dabei die Passwörter für die Ressource im Klartext offenzulegen. Ohne die Passwörter zu sehen, können Benutzer so direkt RDP-, SSH-, Telnet- oder SQL-Konsolen-Verbindungen zu Remote-Ressourcen starten und sich komfortabel automatisch bei Websites und Anwendungen anmelden.

Integration mit AD und LDAP

Für das komfortable Anlegen und die Authentifizierung von Benutzern lässt sich Password Manager Pro mit den zentralen Verzeichnisdiensten Active Directory (AD) oder LDAP integrieren. PMP synchronisiert kontinuierlich mit dem AD und aktualisiert automatisch die User-Datenbank, wenn Benutzer im AD hinzugefügt oder entfernt werden. Außerdem kann die Active-Directory-Authentifizierung auf Password Manager Pro ausgeweitet werden, so dass sich Benutzer mit ihren AD-Daten anmelden können.

Problemloses Anlegen und Löschen von Benutzern:

Password Manager Pro behält die User-Gruppen-Struktur des AD bei. Da die Zugriffsberechtigung für verschiedene Passwörter auf Basis der AD-Gruppen erteilt werden kann, erfolgt auch die Bereitstellung sowie Deaktivierung eines Zugangs entsprechend den Änderungen im Windows-Verzeichnisdienst. So werden die gängigen Sicherheitsrisiken bei diesen Vorgängen vermieden.

Zusätzliche Sicherheitsebene für Passwortfreigabe

Password Manager Pro zieht eine zusätzliche Sicherheitsebene für Passwörter ein, auf der Benutzer einen Freigabeprozess durchlaufen. Dabei müssen die User eine begründete Anfrage an den Administrator stellen – dieser kann vor einer Bewilligung die Anfrage prüfen und unzulässige Anträge ablehnen. Bei Bedarf lassen sich auch zwei Freigabeschleifen vorgeben, was dann die Bewilligung durch zwei oder mehr Administratoren erfordert. Das hilft, den Missbrauch von privilegierten Konten durch böswillige Insider zu vermeiden.

Unsicheren und dauerhaften Zugang vermeiden, wenn User nur zeitweise Zugriff benötigen:

Oft erhalten IT-Mitarbeiter oder Dritte die Möglichkeit, bestimmte Ressourcen temporär zu nutzen, beispielsweise um Fehler zu beheben. In solchen Fällen werden Passwörter oft per E-Mail oder Anruf übermittelt – ein Vorgang, der schnell in Vergessenheit gerät. IT-Mitarbeiter oder gar Außenstehende hätten in diesem Fall jedoch zeitlich uneingeschränkten Zugang zu den betroffenen Ressourcen. Mit Password Manager Pro können Administratoren die Freigabe eines Passworts auf einen bestimmten Zeitraum begrenzen. Nach Ablauf der Zeit wird es automatisch zurückgesetzt, und die Zugriffsberechtigung erlischt.

Vermeiden Sie Abstimmungsprobleme und Änderungskonflikte:

Greifen mehrere Administratoren gleichzeitig auf ein- und dieselbe IT-Ressource zu, kann das Änderungskonflikte und Abstimmungsprobleme nach sich ziehen. Mit Password Manager Pro können Sie bestimmten Benutzern zeitlich begrenzten, exklusiven Zugriff gewähren.

Behalten Sie die Kontrolle über den Zugriff durch Dritte:

Subunternehmer, Zeitarbeiter, Geschäftspartner und Lieferanten zählen zu einer externen Nutzergruppe, die Zugriff auf teils kritische IT-Anlagen benötigt. Damit das möglich ist, müssen sie Zugang zu einem Passwort beantragen. Administratoren können mit Password Manager Pro diesen Zugang zeitlich begrenzen; nach Ablauf wird die Zugriffsberechtigung automatisch entzogen und das Passwort zurückgesetzt. Dieser Prozess gewährleistet absolute Kontrolle über den Zugriff durch Dritte auf unternehmenseigene IT-Ressourcen.

Zugangsbereitstellung und -steuerung

Password Manager Pro kann Passwörter für Remote-IT-Ressourcen automatisch in regelmäßigen Abständen oder bei Bedarf jederzeit zurücksetzen. Das Tool teilt jedem Account dabei ausschließlich starke, einmalige Passwörter zu. Dabei wird über alle physischen, virtuellen und Cloud-Umgebungen hinweg ein breites Spektrum an Endpunkten und Zielsystemen unterstützt.

Schwache und statische Passwörter vermeiden, Hacker-Angriffe abwehren:

Password Manager Pro eliminiert statische, unveränderte Passwörter im ganzen Netzwerk, indem für Remote-Ressourcen automatisch und in regelmäßigen Abständen starke, einmalige Passwörter generiert werden. Das beugt unautorisiertem Zugriff und Diebstahl-Versuchen vor.

Keine statischen Servicekonten:

Systemprogramme nutzen Konten mit besonders weit reichenden Privilegien, um Software-Anwendungs-Services oder -Prozesse auszuführen – hierfür sind bisweilen sogar eigene Zugriffsberechtigungen erforderlich. Die Passwörter solcher Servicekonten sind in der Regel auf „Never Change“ konfiguriert. Denn es ist schwierig, alle abhängigen Services ausfindig zu machen und diese nach der Änderung des Passworts entsprechend zu synchronisieren. Statische Servicekonten sind daher ein beliebtes Einfallstor für Hacker. Password Manager Pro erkennt entsprechende Accounts automatisch: Die Lösung identifiziert die verschiedenen Windows-Server-Komponenten, die über Domain-Konten ausgeführt werden, und weist die jeweiligen Services samt geplanter Aufgaben den entsprechenden Konten zu. Wird das Passwort eines Servicekontos zurückgesetzt, übermittelt Password Manager Pro automatisch die Änderung an alle abhängigen Services, die mit dem Account in Verbindung stehen. Auf diese Weise vermeidet die Lösung Service-Unterbrechungen.

Keine Pass-the-Hash-Attacken:

Domain-Administrator-Konten von Windows verfügen über administrative Zugriffsberechtigungen auf alle Arbeitsplätze, Server und Domain-Controller. Nur ausgewählte Administratoren sollten diese Accounts nutzen. Zudem sollten sie das Konto ausschließlich verwenden, um sich in Domain-Controller-Systemen anzumelden, die so sicher sind wie die Domain-Controller selbst – denn Windows-Systeme weisen leider diverse Schwachstellen gegenüber Pass-the-Hash-Attacken auf.

Mit der Single-Sign-on-Funktion von Windows müssen Benutzer ihre Anmeldedaten samt Passwort nur einmal eingeben: Das Betriebssystem speichert die Login-Informationen in Form von Hash-Werten im Cache. Verschafft sich ein Hacker Zugriff auf ein System, in dem zuvor der Domain-Administrator mit seinen Berechtigungen angemeldet war, gelangt der Angreifer an die gesammelten Hash-Werte. In der Folge ist er in der Lage, unautorisierte Vorgänge durchzuführen.

Als Best-Practice-Ansatz gilt daher: Domain-Administrator-Konten ausschließlich zur Anmeldung an Domain-Controllern nutzen! Falls der Zugriff auf ein anderes System dringend notwendig ist, sollte der Zugang für die einmalige Nutzung samt Zurücksetzen des Passworts konfiguriert sein. Auch wenn auf Domain-Administrator-Konten von vertrauenswürdigen Systemen mit Bedacht zugegriffen wird, ist es empfehlenswert, die Berechtigungen regelmäßig zu variieren. Password Manager Pro unterstützt Sie bei dieser Aufgabe – und hilft so, Pass-the-Hash-Attacken zu verhindern.

APIs für das Passwort-Management von “Application-to-Application” und “Application-to-Database”

Password Manager Pro stellt drei Arten von Schnittstellen (APIs) für das Application-to-Application-Passwort-Management zur Verfügung: SSH-CLI, XML-RPC und REST. Anwendungen können so direkt Anfragen an Password Manager Pro stellen, um Berechtigungen zu erhalten.

Eliminieren Sie fest codierte Berechtigungen:

In der Regel benötigen zahlreiche Anwendungen Zugriff auf Datenbanken und andere Applikationen, um unternehmensbezogene Informationen abzufragen. Dieser Kommunikationsprozess erfolgt üblicherweise automatisch, indem die Berechtigung der Anwendung als Klartext in Konfigurationsdateien und -skripte eingebettet wird. Administratoren empfinden es meist als schwierig, diese Passwörter zu identifizieren, zu ändern und zu verwalten. Sie bleiben somit über lange Zeiträume gleich, was den unberechtigten Zugriff auf sensible Systeme erleichtern kann. Hart codierte Berechtigungen vereinfachen die Arbeitsabläufe für die Techniker, stellen jedoch auch für Hacker ein mögliches Einfallstor dar.

Mit sicheren APIs für das Passwort-Management von Application-to-Application und Application-to-Database verzichtet Password Manager Pro auf die Praxis fest codierter Passwörter. Die Zugangsberechtigungen wandern nicht mehr in Konfigurationsdateien, sondern werden in der Datenbank von Password Manager Pro gespeichert. Benötigt eine Anwendung eine Verbindung zu einer anderen beziehungsweise zu einer Datenbank, kann sie einfach über die APIs eine Anfrage an Password Manager Pro stellen und die erforderlichen Passwörter abrufen. Damit lassen sich – ohne umfangreiche manuelle Updates – bewährte Sicherheitspraktiken anwenden, etwa periodische passwortrichtlinienkonforme Änderungen.

Sicherheitsrisiken in DevOps-Umgebungen reduzieren:

DevOps-Umgebungen umfassen verschiedene Bereiche eines Software-Lebenszyklus wie Sandbox, Entwicklung, Unit Tests, Integration, Qualitätssicherung, Akzeptanztest, Produktion und Disaster Recovery. Darüber hinaus erfordern sie einen automatisierten Zugriff auf privilegierte Identitäten durch verschiedene Stakeholder. Anwendungen, Skripte und Datenbanken, die in DevOps-Umgebungen laufen, setzen einen Zugriff auf privilegierte Identitäten ohne menschliches Zutun voraus. Wird dieser Zugang über fest codierte Berechtigungen ermöglicht, stellt das die gefährlichste und risikoreichste Herangehensweise dar. Die APIs von Password Manager Pro verschaffen einen automatisierten Zugriff auf die Passwörter von autorisierten Anwendungen und unterstützen zudem standardisierte Passwort-Praktiken. So lassen sich Sicherheitsprobleme in DevOps-Umgebungen vermeiden. Ohne fest codierte Berechtigungen.

Fernzugriff & Management von privilegierten Sitzungen

Autorisierte Benutzer können RDP-, SSH-, Telnet- oder SQL-Sitzungen komfortabel direkt über jeden HTML5-kompatiblen Browser starten. Dazu sind weder Endpunkt-Agenten, noch Browser-Plug-Ins oder Hilfsprogramme nötig: Der Password-Manager-Pro-Server tunnelt die Verbindungen, so dass keine direkte Verknüpfung zwischen dem Endgerät eines Nutzers und dem Host nötig ist.

Die getunnelten Verbindungen sorgen zudem für extrem hohe Sicherheit, da die Passwörter zum Start der Remote-Verbindung nicht im Browser des Benutzers vorhanden sein müssen. Sitzungen, die von der webbasierten PMP-Oberfläche gestartet werden, lassen sich aufzeichnen und archivieren und so auch als Beweismittel für forensische Audits verwenden. Zusätzlich können Administratoren mit Password Manager Pro privilegierte Sitzungen überwachen, die andere Benutzern gestartet haben.

Weniger Risiken bei der Vergabe eines Remote-Zugangs an Dritte:

Unternehmen können mit Password Manager Pro die Risiken eines Identitätsdiebstahls durch Außenstehende senken. Dazu gilt es, Passwörter, die mit Dritten geteilt wurden, zu schützen und regelmäßig zu ändern.

Mit der richtigen Landing-Server-Konfiguration das Angriffsrisiko an Endpunkten reduzieren:

In hochsicheren Umgebungen wie Rechenzentren kann der Fernzugriff auf sensible Endpunkte über einen Jump Server gewährt werden. Password Manager Pro zentralisiert das Management aller Berechtigungen einschließlich der Jump Server und regelt den Zugriff. Die passende Landing-Server-Konfiguration verhindert dabei, dass Endpunkte durch unsichere Verbindungen zu Geräten an Standorten von Dritten infiziert werden.

Böswillige oder verdächtige Aktivitäten durch zweifache Kontrollen verhindern:

Hochsensible privilegierte Sitzungen, die Dritte oder interne Benutzern gestartet haben, können in Echtzeit verfolgt und bei verdächtigen Aktivitäten beendet werden.

Leugnen zwecklos:

Im Fall von Sicherheitsverstößen oder -konflikten können Dritte oder interne Administratoren nicht leugnen, bestimmte Aktivitäten durchgeführt zu haben: Password Manager Pro zeichnet alle privilegierten Sitzungen vollständig auf.

Audit, Echtzeit-Management, Berichte

Password Manager Pro zeichnet jede Aktion eines Benutzers auf und erstellt zusätzlich textbasierte Protokolle. Bei passwortrelevanten Ereignissen – Zugriffen, Änderungen, Löschvorgängen, geänderten Freigabeberechtigungen etc. – warnt und informiert das Tool in Echtzeit.

Vermeiden Sie Verantwortlichkeitskonflikte:

Administrative Konten sind normalerweise nicht an einen Benutzer gebunden und werden vor allem in geteilten Umgebungen genutzt. Treten Probleme auf, stellt sich daher beinahe zwangsläufig die Frage nach Verantwortlichkeiten. Kommt hingegen Password Manager Pro als zentrales Passwort-Repository zum Einsatz, können Administratoren ausschließlich über PMP und damit immer nachvollziehbar Kenntnis über Passwörter erlangen. Von Password Manager Pro generierte Audit-Trails ermöglichen es außerdem, den Zugang zu einzelnen Personen zurückverfolgen.

Bekämpfung von intelligenten, fortdauernden Bedrohungen:

Intelligente Cyber-Attacken halten in der Regel länger an – daher ist es sinnvoll, Daten verschiedener IT-Assets mit den privilegierten Zugriffsdaten von Password Manager Pro zu korrelieren. Dieser generiert Syslog-Meldungen, die an SIEM-Lösungen übermittelt und in Korrelation zu weiteren Ereignissen im Unternehmen gebracht werden können. So lassen sich Angriffe aufdecken, noch während sie stattfinden, oder sie lassen sich sogar von Anfang an verhindern.

Kommen Sie dem Missbrauch privilegierter Konten durch böswillige Insider zuvor:

Password Manager Pro hilft Unternehmen durch Warnmeldungen und Benachrichtigungen in Echtzeit, unberechtigte Aktivitäten und den Missbrauch privilegierter Konten durch böswillige Insider aufzudecken.

G2 CROWD KUNDENSTIMMEN

Ein großartiges Produkt, erstklassiges Support Team!

★★★★★

Das Preismodell ist sehr überzeugend, das Beste, das ich kenne. Das Tool funktioniert einwandfrei, bei Problemen steht das Support-Team kompetent zur Seite. Sie kennen ihr eigenes Produkt und helfen, wo sie nur können. Sie versorgten uns sogar innerhalb eines Tages mit einem eigenen Patch. So einen Kundendienst habe ich noch nie erlebt. Ich bin ein glücklicher und zufriedener Kunde!

Martijn Dirkx,
System Administrator,
SeaChange International, Niederlande

Eine exzellente Ressource. Einfach zu bedienen und zu warten.

★★★★★

Es ist großartig, die Passwörter von allen Geräten, externen Sites und internen Anwendungen auf einem zentralen Server aufzubewahren. Dieser Server ist sogar Teil unseres Disaster-Recovery-Konzepts.

Steven.R.McEvoy,
Senior Systems Analyst, Christie Digital Systems, Kanada

Eine leistungsstarke Anwendung für das Management von Unternehmens-Passwörtern.

★★★★☆

Mit Password Manager Pro konnten wir unsere Probleme mit den administrativen Konten endlich lösen. Das zentrale Passwort-Management, die automatisierten Passwort-Resets und das Reporting sind einige der Funktionen, die uns am meisten überzeugt haben.

Said Youssef,
Senior Security Officer,
Chisholm Institute, Australien

Technische Daten

Erkennung: Agentenlos

Passwort-Zurücksetzung: Agentenbasiert, agentenlos

Authentifizierung: Active Directory, LDAP, RADIUS, SAML

Verschlüsselungsalgorithmus: AES-256

Produkt-Installation: Windows, Linux (32-bit und 64-bit)

Back-End Datenbank: PostgreSQL (gebündelt), MS SQL, MySQL

Unterstützte APIs: RESTful API, XML RPC, SSH CLI

Unterstützte Plattformen für Erkennung, Fernzugriff und Passwort-Zurücksetzung:

A) Betriebssysteme

- Windows (Local-1, Domain-, und Service-Accounts)
- Linux, UNIX, und Mac OS
- Solaris
- IBM AIX

B) Datenbanken

- MS SQL
- MySQL
- Oracle
- Sybase ASE

C) Virtuelle Plattformen

- VMWare ESXi

D) Netzwerkgeräte

- Juniper Netscreen
- HP ProCurve
- HP iLO
- Cisco devices (IOS, CatOS, PIX)
- Sun Oracle (ALOM, ILOM, XSCF)

E) Directory-Services

- Active Directory
- LDAP-konformer Server

F) Cloud-Infrastruktur

- AWS - IAM
- Google Apps
- Microsoft Azure
- Rackspace

Vorkonfigurierte Integration

- Active Directory/LDAP-konforme Services
- SIEM-Integration (SNMP-Traps)
- Ticket-Systeme für Unternehmen (ServiceDesk Plus, ServiceNow, und mehr)
- SAML 2.0 integration

Haftungsausschluss

Die vollständige Einhaltung der DSGVO-Vorschriften erfordert eine Vielzahl von Lösungen, Prozessen, Menschen und Technologien. Wie ausgeführt ist die Automatisierung des privilegierten Zugangsmanagements nur ein erster Schritt für Compliance im Sinne der DSGVO. Zusammen mit anderen geeigneten Maßnahmen trägt das privilegierte Zugangsmanagement dazu bei, die IT-Sicherheit zu erhöhen und Verletzungen der Datensicherheit vorzubeugen. Das oben stehende und hinterlegte Material dient ausschließlich der Information und ist keine juristische Beratung im Hinblick auf die Compliance mit der DSGVO. ManageEngine übernimmt hinsichtlich der in diesem Material enthaltenen Informationen keine Garantien, weder ausdrücklich noch stillschweigend oder gesetzlich vorgeschrieben.

Bildnachweis:

Seite 1: © Sergey Nivens / Fotolia.com
Seite 2: © kupicoo / iStock.com
Seite 6: © sdecoret / Fotolia.com
Seite 9: © Georgijevic / iStock.com
Seite 15: © deepadesigns / Shutterstock.com
Seite 17: © Sergey Nivens / Shutterstock.com
Seite 19: © Wright Studio / Shutterstock.com
Seite 23: © Sergey Tarasov / Shutterstock.com
Seite 25: © shock / Fotolia.com
Seite 26: © Yuri Arcurs / Fotolia.com

Ihr deutscher Partner:
MicroNova AG
Unterfeldring 17
D-85256 Vierkirchen
Telefon: +49 81 39 / 93 00 - 456
sales-ManageEngine@micronova.de
www.manageengine.de/passwordmanagerpro

Zoho Corporation
4141 Hacienda Drive Pleasanton
CA 94588, USA
Telefon: +1-925-924-9500
Fax: +1-925-924-9600
Email: sales@manageengine.com
www.manageengine.com/passwordmanagerpro