EXPERTS IN IDENTITY.
ACCESS. GOVERNANCE.

Praxis-Guide

Privileged Access Management

Ein Leitfaden zur Einführung von PAM-Strategien und -Lösungen.

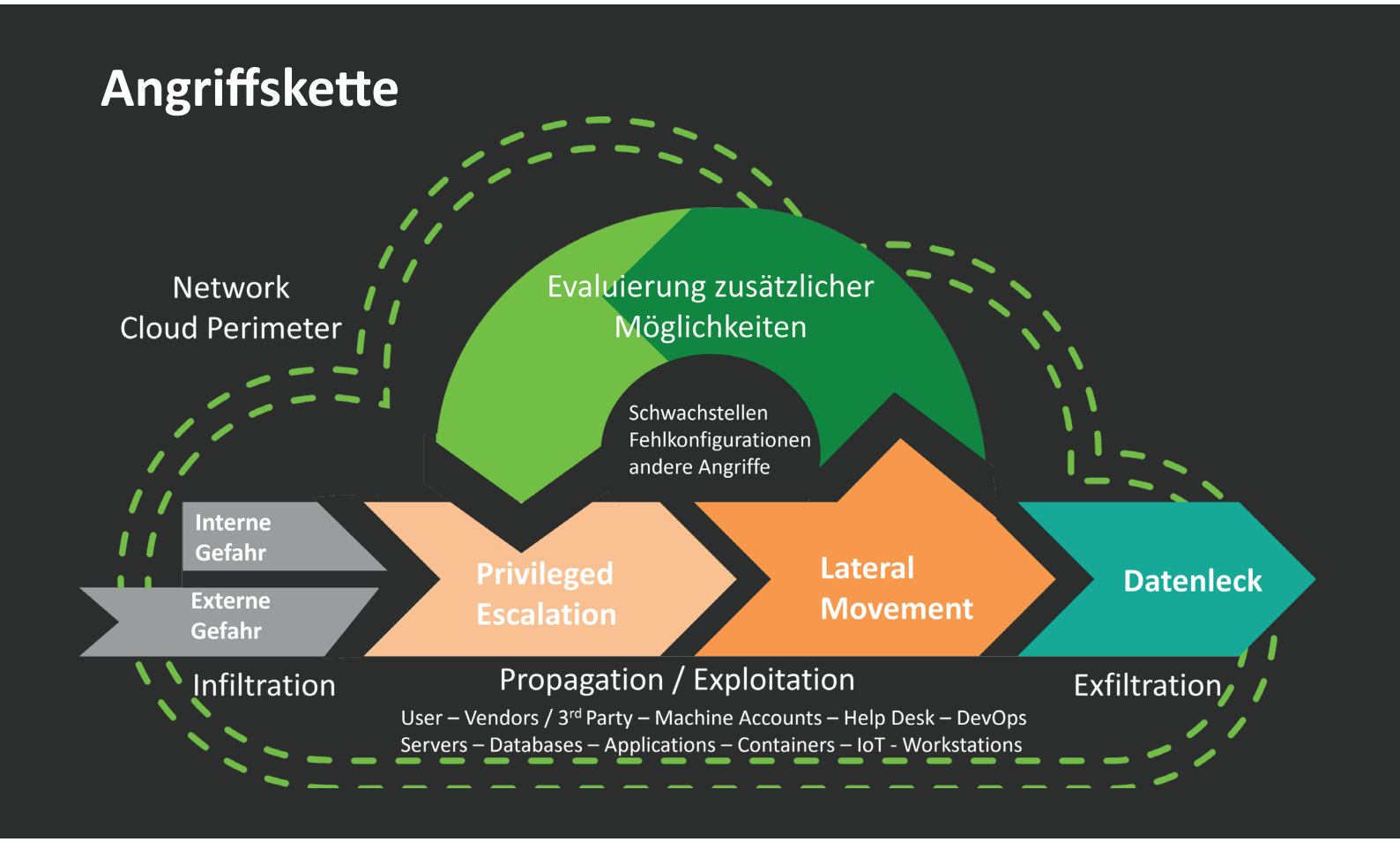
- # Schutz vor Datendiebstahl
- # Automatisierte Passwortverwaltung
- # Kontrolle privilegierter Zugriffe

1. Einleitung

Privileged Access Management (PAM) ist ein entscheidendes Thema für Unternehmen jeder Grösse. Als wichtige Sicherheitsmassnahme hilft es den Schutz sensibler Daten und Systeme zu gewährleisten und sich gegen interne und externe Bedrohungen zu wappnen.

In diesem Praxis-Guide für **Privileged Access Management**-Lösungen zeigen wir auf, warum es für die IT-Sicherheit so wichtig ist ein PAM-System zu betreiben und wie es eingesetzt werden kann, um Risiken zu minimieren und die Einhaltung von Compliance-Richtlinien zu gewährleisten.

Dabei betrachten wir verschiedene PAM-Lösungen, deren Funktionen und praktische Schritte zur Implementierung in Unternehmen.



In der heutigen digitalen Welt ist die Verwaltung und Kontrolle des Zugriffs auf IT-Ressourcen entscheidend, um Sicherheitsverletzungen vorzubeugen und um zu verhindern, dass unbefugte Benutzer oder Cyberkriminelle auf vertrauliche Informationen zugreifen können.

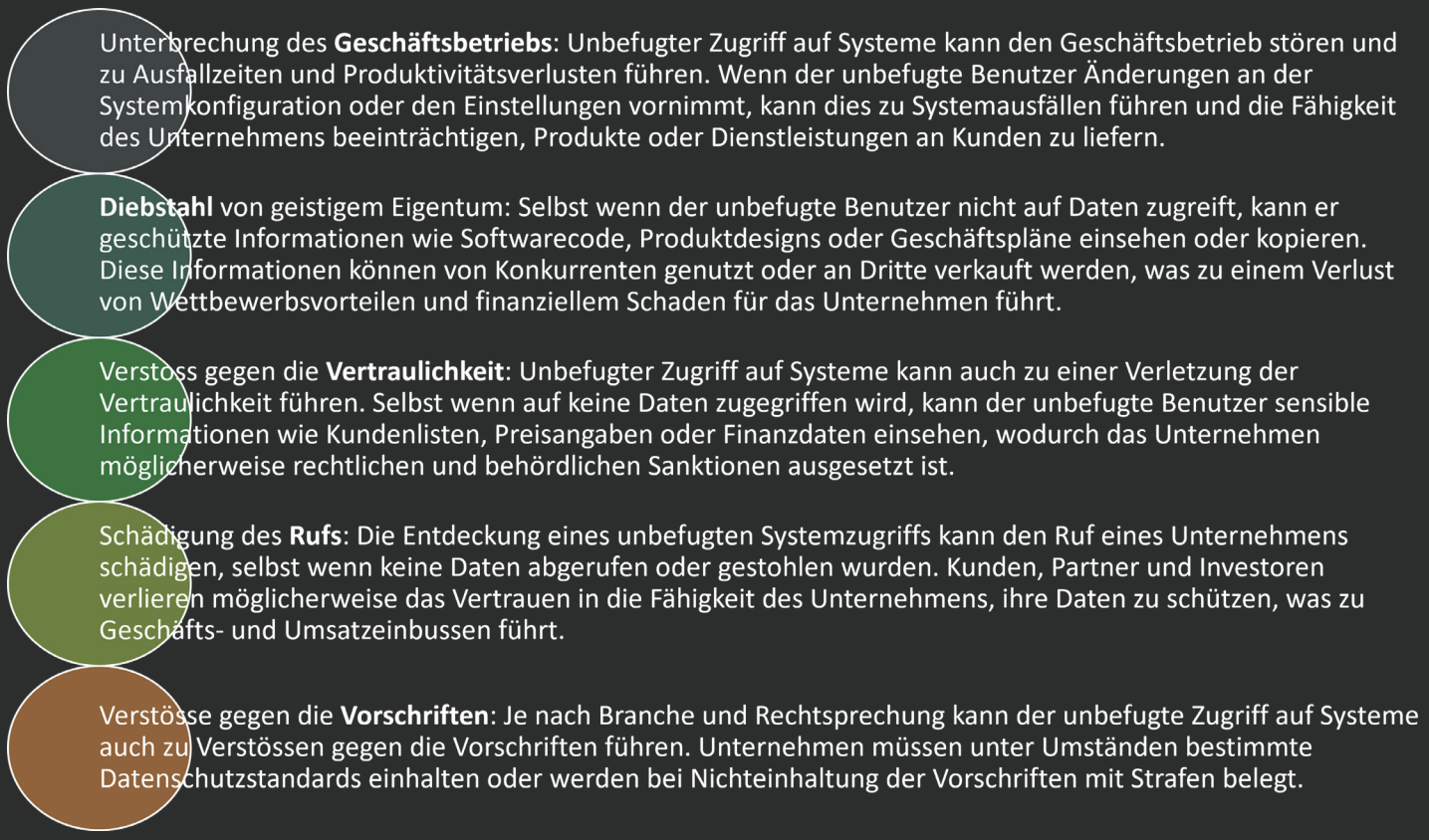
Dabei stehen die hochprivilegierten Benutzer und Systemberechtigungen im Fokus, da sie das grösste Schadensrisiko darstellen. Unternehmen sind gezwungen, privilegierte Konten und Zugangsrechte so zu verwalten, dass diese nur für berechtigte Benutzer zur Verfügung stehen.

Durch die Implementierung einer effektiven Privileged Access Management-Lösung können Unternehmen ihre Sicherheit erhöhen, indem sie Nachvollziehbarkeit und Kontrolle über administrative Sitzungen herstellen und gleichzeitig Bedrohungsschutzmassnahmen wie Zugriffssteuerung und Benutzeranalyse in ihre IT-Systeme integrieren.

2. Warum ist Privileged Access Management (PAM) wichtig?

Privileged Access Management (PAM) ist wichtig, um IT-Ressourcen vor Cyberangriffen zu schützen und um Compliance-Anforderungen zu erfüllen.

- Laut einer Studie von CyberArk sind **74 %** der Sicherheitsverletzungen auf den Missbrauch von privilegiertem Zugang zurückzuführen.
- Eine Umfrage von Thycotic ergab, dass **52 %** der Unternehmen über keine Strategie für die Verwaltung privilegierter Zugriffe verfügen.
- Dieselbe Umfrage ergab auch, dass **70 %** der Befragten der Meinung sind, dass die Verwaltung privilegierter Zugriffe für ihr Unternehmen sehr wichtig oder entscheidend ist.
- Laut Gartner werden bis 2025 **80 %** der Unternehmen Tools und Prozesse für das Privileged Access Management einsetzen um den Zugriff auf Infrastruktur und Anwendungen zu kontrollieren, gegenüber **50 %** im Jahr 2020.



2.1 Schutz vor Cyberangriffen

Privileged Access Management (PAM) spielt eine entscheidende Rolle beim Schutz vor Cyberangriffen, indem sie den Zugriff auf kritische IT-Ressourcen und sensible Daten kontrolliert und überwacht.

Eine effektive PAM-Lösung identifiziert privilegierte Konten, wie zum Beispiel Systemadministratoren oder Führungskräfte und stellt sicher, dass nur autorisierten Benutzern der Zugang zu diesen Konten gewährt wird.

Dies begrenzt die Angriffsfläche für Hacker und verhindert, dass sie unbefugt auf vertrauliche Informationen oder Systeme zugreifen können.

Ein Beispiel für die Bedeutung von PAM im Bereich der Cyber-Sicherheit: Durch den Angriff auf einen Einzelhändler erlangten Hacker Zugang zum Netzwerk des Unternehmens, indem sie Anmeldeinformationen eines Lieferanten nutzten, der nicht ausreichend abgesicherte privilegierte Zugangsrechte hatte.

Durch die erfolgreiche Kompromittierung dieser Anmeldeinformationen konnten die Angreifer Daten von Millionen von Kunden stehlen, was zu enormen finanziellen Verlusten und einem erheblichen Imageschaden geführt hat. Eine PAM-Lösung hätte in diesem Szenario dabei helfen können, den unbefugten Zugriff auf das Netzwerk zu erkennen sowie rechtzeitig Gegenmassnahmen einzuleiten. Darüber hinaus sind Cyberangriffe nicht immer nur auf externe Bedrohungen beschränkt. Interne Bedrohungen, wie fahrlässige oder böswillige Mitarbeitende, können ebenso verheerende Folgen für ein Unter-nehmen haben.

PAM-Lösungen können auch hierbei helfen, diese Risiken zu minimieren und sicherzustellen, dass nur wirklich benötigte Berechtigungen für den jeweiligen Verantwortungsbereich eines Mitarbeitenden vergeben werden. Somit wird auch die Gefahr von Datenlecks oder Fehlkonfigurationen durch menschliches Versagen verringert.

2.2 Erfüllung von Compliance-Anforderungen

Die Erfüllung von Compliance-Anforderungen ist ein wesentlicher Aspekt für Unternehmen, um sicherzustellen, dass ihre IT-Ressourcen und -Systeme im Einklang mit geltenden Gesetzen, Vorschriften und Sicherheitsstandards stehen.
Zum Beispiel helfen PAM-Lösungen Organisationen dabei, den Grundsatz der minimalen Berechtigungen (Least-Privilege-Prinzip) umzusetzen, indem sie sicherstellen, dass Mitarbeitende und Systemadministratoren nur Zugang zu den Ressourcen haben, die für ihre Arbeit unbedingt erforderlich sind.
Ein weiterer wichtiger Aspekt von Compliance-Anforderungen ist die Nachvollziehbarkeit von administrativen Sitzungen. Dies bedeutet, dass alle Aktionen von privilegierten Benutzern im System genauestens protokolliert und überwacht werden müssen, um sicherzustellen, dass keine unerwünschten Änderungen oder Manipulationen vorgenommen werden.
PAM-Lösungen helfen hierbei, indem sie vollständige Auditierungs- und Überwachungsfunktionen anbieten, die es Sicherheitsverantwortlichen ermöglichen, einen detaillierten Überblick über alle privilegierten Zugriffe und Aktivitäten innerhalb ihrer Infrastruktur zu erhalten.

Einige der wichtigsten regulatorischen Anforderungen, die PAM unterstützt, sind:

- **ISO/IEC 27001:** Dieser internationale Standard für Informationssicherheitsmanagementsysteme (ISMS) bietet einen Rahmen für die Sicherung von vertraulichen Informationen. PAM-Lösungen unterstützen die Einhaltung von ISO/IEC 27001, indem sie den Zugriff auf kritische Systeme und Daten kontrollieren und überwachen.

- **Health Insurance Portability and Accountability Act (HIPAA):** HIPAA ist ein US-Gesetz, das den Schutz und die Vertraulichkeit von Patientendaten in der Gesundheitsbranche regelt. PAM-Lösungen helfen, den Zugriff auf geschützte Gesundheitsinformationen (PHI) zu kontrollieren und nachzuverfolgen.

- **Sarbanes-Oxley Act (SOX):** Dieses US-Gesetz zielt darauf ab, Betrug in börsennotierten Unternehmen durch Verbesserung der Transparenz und Corporate Governance zu verhindern. PAM-Lösungen unterstützen die Einhaltung der SOX-Anforderungen, indem sie den Zugriff auf Finanzsysteme und -informationen verwalten.

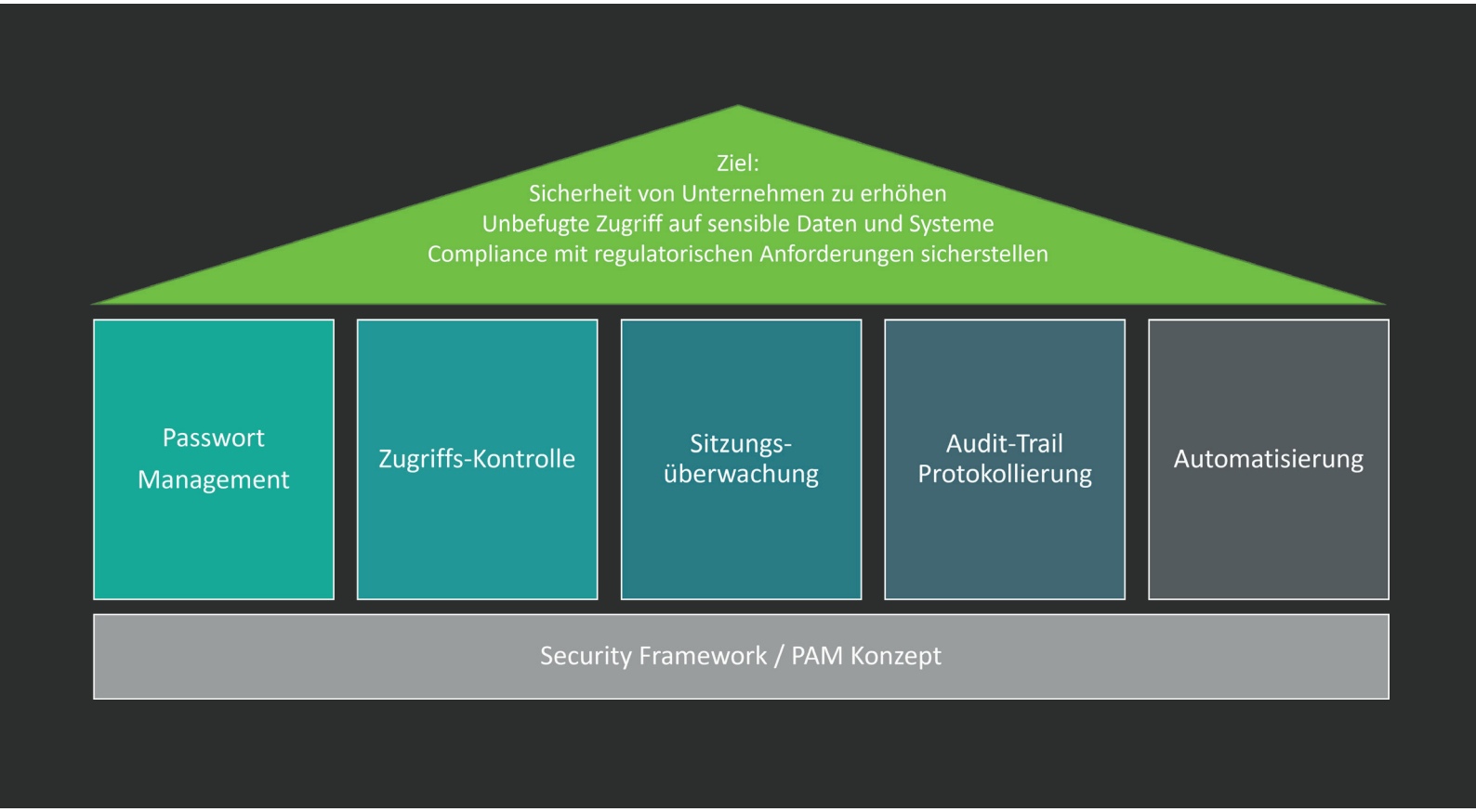
- **Payment Card Industry Data Security Standard (PCI-DSS):** PCI-DSS ist ein Sicherheitsstandard für Organisationen, die Kreditkartentransaktionen verarbeiten. PAM-Lösungen unterstützen die Einhaltung von PCI-DSS, indem sie den Zugriff auf Kreditkarteninformationen und andere sensible Daten beschränken und protokollieren.

- **Datenschutzgesetze:** Datenschutzgesetze regeln generell den Schutz von Daten, insbesondere personenbezogener Informationen. PAM-Lösungen unterstützen die Einhaltung, indem sie den Zugriff auf personenbezogene Daten verwalten und protokollieren.

- **Datenschutz-Grundverordnung (DSGVO):** Die DSGVO ist eine umfassende Datenschutzverordnung der Europäischen Union, die den Schutz personenbezogener Daten von EU-Bürgern regelt. PAM-Lösungen unterstützen die Einhaltung der DSGVO, indem sie den Zugriff auf personenbezogene Daten verwalten, protokollieren und kontrollieren.

3. Funktionen von PAM-Lösungen

PAM-Lösungen bieten verschiedene Funktionen, einschliesslich Passwort-Management, Zugriffsmanagement, Überwachung und Auditierung sowie Automatisierung von Prozessen, um die Sicherheit und Compliance von privilegierten Accounts zu gewährleisten.



3.1 Passwort-Management

Der Schutz von Passwörtern ist ein zentrales Element des Privileged Access Managements. Ohne ein angemessenes Passwort-Management kann jederzeit ein unbefugter Zugriff auf sensible Daten und Systeme erfolgen.

PAM-Lösungen bieten verschiedene Funktionen, um ein effektives Passwort-Management zu gewährleisten. So können beispielsweise Passwörter automatisch generiert, regelmässige Passwort-Änderungen durchgesetzt und die Anzahl der möglichen fehlgeschlagenen Anmeldeversuche eingeschränkt werden. Doch nicht nur die technischen Aspekte sind wichtig, auch die Mitarbeitende müssen sensibilisiert werden. Regelmässige Schulungen und Awareness-Kampagnen können hier einen wichtigen Beitrag leisten. Eine einfache Möglichkeit zur Verbesserung des Passwort-Managements ist zudem die Einführung von Single-Sign-On Lösungen, welche es den Nutzern ermöglicht, sich mit einem einzigen Zugang zum System anzumelden, ohne sich jedes Mal an verschiedenen Orten anmelden zu müssen.

Ein solides Passwort-Management ist somit eine wichtige Basis für ein effektives PAM und sollte in keiner Sicherheitsstrategie fehlen.

3.2 Zugriffsmanagement

Zugriffsmanagement ist eine wichtige Funktion von Privileged Access Management (PAM)-Lösungen. Es bezieht sich auf die Kontrolle und Verwaltung des Zugriffs auf privilegierte Konten und Systeme. Mit PAM-Lösungen können IT-Verantwortliche den Zugang zu IT-Ressourcen einschränken und sicherstellen, dass nur autorisierte Benutzer mit den entsprechenden Berechtigungen darauf zugreifen können.

Eine effektive Zugriffsverwaltung kann dazu beitragen, das Risiko von Missbrauch oder unbefugtem Zugriff auf sensible Daten oder kritische Systeme zu reduzieren. Beispielsweise kann eine PAM-Lösung eine Überprüfung der Benutzeridentität erfordern, bevor privilegierte Konten zugänglich sind. Ein weiteres Beispiel ist das Implementieren von First-in-First-out-Zugangsbeschränkungen, um sicherzustellen, dass nur eine begrenzte Anzahl von Benutzern gleichzeitig privilegierten Zugriff erhält.

PAM-Lösungen bieten auch Funktionen zur Überwachung und Auditierung von privilegierten Sitzungen sowie zur Automatisierung von Prozessen. Die Überwachung ermöglicht es IT-Verantwortlichen, die Aktivitäten der Benutzer in Echtzeit zu verfolgen und ungewöhnliche Aktivitäten auf privilegierten Konten zu erkennen. Die Automatisierung kann wiederum dazu beitragen, menschliche Fehler bei der Verwaltung von Zugriffsrechten zu minimieren und repetitive Aufgaben zu vereinfachen.

3.3 Überwachung und Auditierung

Eine der wichtigsten Funktionen von Privileged Access Management (PAM)-Lösungen ist die Überwachung und Auditierung von privilegierten Accounts. Durch die Überwachung kann das Systemadministratoren-Team ungewöhnliche Aktivitäten oder verdächtige Zugriffsversuche anhand von Benutzeranalyse und Entitätsverhaltensanalyse erkennen. So kann ein möglicher Cyberangriff frühzeitig erkannt und verhindert werden.

Die Auditierung ermöglicht IT-Verantwortlichen eine lückenlose Nachvollziehbarkeit und Kontrolle über administrative Sitzungen, Zugriffsverwaltung und Passwort-Management. IT-Sicherheitsrichtlinien und Compliance-Anforderungen können damit erfüllt werden. Eine PAM-Lösung bietet hierbei auch Schutz sensibler Daten durch Zugriffsbeschränkungen, Benutzerrechte und -beschränkungen sowie Vertraulichkeit und Überwachung. Zusammenfassend lässt sich sagen, dass Überwachung und Auditierung ein unverzichtbarer Bestandteil jeder PAM-Lösung sind, um IT-Ressourcen effektiv zu schützen und Compliance-Anforderungen zu erfüllen.

3.4 Automatisierung von Prozessen

PAM-Lösungen bieten nicht nur Zugriffs- und Passwort-Management, sondern können auch die Automatisierung von Prozessen umfassen.

Diese Funktion hilft Unternehmen, Zeit und Kosten zu sparen sowie die Effizienz zu steigern. Ein Beispiel für diese Automatisierung ist die automatische Erstellung von Berichten oder Benachrichtigungen bei unautorisierten Zugriffen auf privilegierte Konten. Dies kann dazu beitragen, potenzielle Probleme schnell zu identifizieren und zu lösen.

Ein weiteres Beispiel für die Automatisierung von Prozessen ist die automatische Rotation von Passwörtern für privilegierte Konten, um den Schutz vor Cyberangriffen zu erhöhen.

Die Passwortrotation kann so eingestellt werden, dass sie regelmässig erfolgt und automatisch durchgeführt wird, ohne dass ein Systemadministrator eingreifen muss. Dadurch wird sichergestellt, dass Passwörter regelmässig geändert werden und dass ein sicherer Zugang zu den privilegierten Konten gewährleistet ist.

Insgesamt bietet die Automatisierung von Prozessen in PAM-Lösungen viele Vorteile und kann Unternehmen dabei helfen, ihre IT-Ressourcen effizienter zu nutzen und gleichzeitig die Sicherheit zu erhöhen.

Checkliste für PAM

Definieren: Definieren Sie, was „privilegierter Zugriff“ bedeutet, und legen Sie fest, was ein privilegiertes Konto für Ihr Unternehmen ist. Bestimmen Sie weiter, welche IT-Systemberechtigungen als privilegiert betrachtet werden sollen.

Entdecken: Identifizieren Sie Ihre privilegierten Konten und implementieren Sie eine kontinuierliche Erkennung, um die Ausbreitung privilegierter Konten einzudämmen, potenziellen Insidermissbrauch zu identifizieren und externe Bedrohungen aufzudecken. Es empfiehlt sich hierfür der Einsatz von PAM-Lösungen mit einer kontinuierlichen Scan-Funktion, welche alle Anlagen und Anwendungen für die Katalogisierung und Eingliederung von privilegierten Accounts und Systemberechtigungen erfasst.

Verwalten und Schützen: Proaktives Verwalten und Kontrollieren des Zugriffs auf privilegierte Konten durch das Planen und Durchsetzen von Kennwortrotationen, Prüfen, Analysieren und Verwalten einzelner privilegierter Sitzungsaktivitäten.

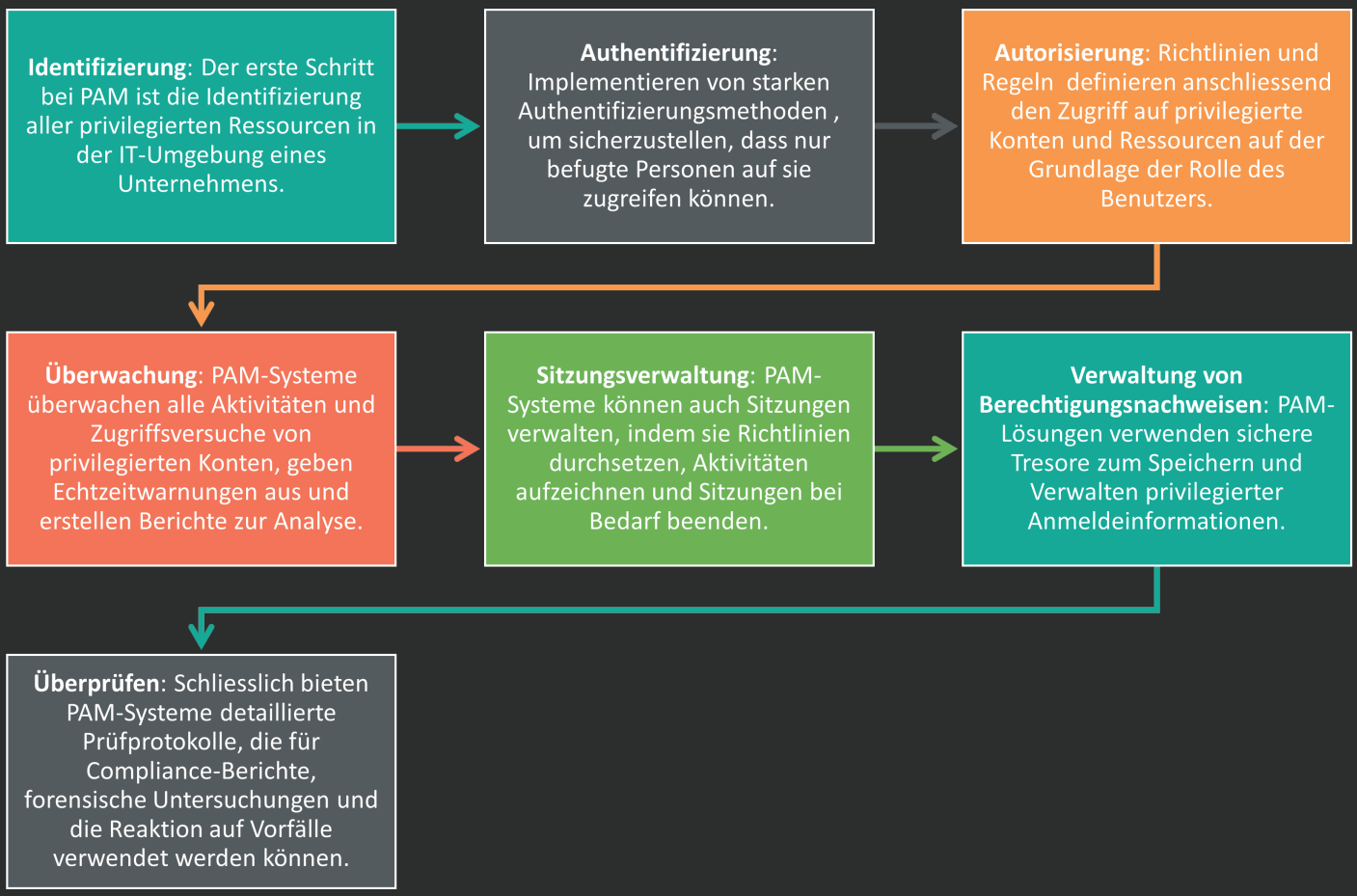
Monitor: Überwachen und Aufzeichnen von Aktivitäten privilegierter Konten, stellen Sie sicher, dass Sie den Zugriff und die Aktivitäten Ihrer privilegierten Konten in Echtzeit einsehen, um mutmassliche Konto Kompromittierungen und potenziellen Benutzermissbrauch zu erkennen.

Reagieren: Ergreifen Sie Massnahmen, um kompromittierte Konten und Systeme auf der Grundlage definierter Richtlinien und Informationen zu Sicherheitsverletzungen zu schützen.

Überprüfung und Prüfung: Helfen Sie bei der Identifizierung ungewöhnlicher Verhaltensweisen, die auf eine Verletzung oder einen Missbrauch hinweisen können, indem Sie kontinuierlich beobachten, wie privilegierte Konten verwendet werden.

4. Best Practices für die Implementierung von PAM-Lösungen

Um eine erfolgreiche Implementierung von PAM-Lösungen zu gewährleisten, ist es wichtig, privilegierte Accounts zu identifizieren, Least-Privilege-Prinzipien umzusetzen und Mitarbeitende zu schulen. **Erfahren Sie hier mehr über bewährte Verfahren bei der Umsetzung von PAM-Lösungen.**



4.1 Definieren und Identifizieren von Privilegierten Accounts

Die Identifizierung privilegierter Accounts ist ein wichtiger Bestandteil des Privileged Access Managements (PAM). Hierbei geht es darum, alle Benutzerkonten und IT-Systemberechtigungen zu identifizieren, die über erhöhte Berechtigungen verfügen und damit Zugriff auf besonders sensible Daten und Systeme ermöglichen. Oft handelt es sich dabei um administrative Konten wie beispielsweise das des Systemadministrators, aber auch um Konten von Service-Accounts oder externen Partnern.

Es ist wichtig, alle privilegierten Accounts zu identifizieren, da diese ein höheres Risiko für Cyberangriffe darstellen als normale Benutzerkonten. Hacker versuchen oft, sich Zugang zu diesen Konten zu verschaffen, um an vertrauliche Informationen zu gelangen oder Schaden durch Manipulation des Systems anzurichten. Deshalb ist es unabdingbar, diese Konten genauestens zu identifizieren und ihre Zugriffsrechte und Aktivitäten genau zu überwachen.

Um privilegierte Accounts erfolgreich identifizieren zu können, sollten Unternehmen zunächst eine Bestandsaufnahme aller Konten durchführen. Anschliessend können sie entscheiden, welche Konten als privilegiert eingestuft werden und damit einer erhöhten Überwachung unterliegen sollten. Durch eine effektive Identifizierung von privilegierten Accounts können Unternehmen ihre IT-Sicherheit erhöhen und potenzielle Risiken reduzieren.

4.2 Implementierung von Least-Privilege-Prinzipien

Ein wichtiger Bestandteil der Implementierung von Privileged Access Management-Lösungen ist die Anwendung des Least-Privilege-Prinzips. Dabei werden den Mitarbeitenden nur die notwendigen Berechtigungen für ihre Arbeit zugewiesen, um unbeabsichtigte oder böswillige Schäden an kritischen IT-Ressourcen zu verhindern. Beispielsweise sollte ein Mitarbeitender im Finanzbereich nur Zugriff auf Finanzdaten haben, während ein Systemadministrator nur über die notwendigen Berechtigungen verfügen sollte, um kritische Systeme zu warten.

Die Umsetzung des Least-Privilege-Prinzips kann jedoch eine Herausforderung darstellen, da es notwendig ist, alle privilegierten Accounts sorgfältig zu überprüfen und einzuschränken. Eine effektive Methode zur Identifizierung dieser Accounts ist die Durchführung einer gründlichen Inventarisierung, bei der es wichtig ist, auch die verschiedenen Zugangsrechte aufzunehmen. Darüber hinaus sollten Unternehmen auch ihre Mitarbeitenden schulen und informieren, wie sie das Least-Privilege-Prinzip erfolgreich anwenden können.

Insgesamt ist das Implementieren von Least-Privilege-Prinzipien ein wichtiger Schritt bei der Sicherung von privilegierten Zugängen in Unternehmen. Es ist ein unverzichtbarer Bestandteil der Risikomanagementstrategie und trägt dazu bei, dass sensible Daten sowie kritische IT-Ressourcen geschützt werden.

4.3 Schulung von Mitarbeitenden

Wenn es um Privileged Access Management (PAM) geht, sind Mitarbeitende der Schlüssel zur erfolgreichen Implementierung. Eine gründliche Schulung ist unerlässlich, um sicherzustellen, dass alle Mitarbeitende die Notwendigkeit von PAM verstehen und die Verantwortung für die Verwaltung privilegierter Konten übernehmen.

Die Schulung sollte sich auf die Identifikation privilegierter Konten, die Umsetzung von Least-Privilege-Prinzipien und die Überwachung von Zugriffen konzentrieren. Beispielsweise sollten Mitarbeitende lernen, wie sie verdächtige Aktivitäten in Zusammenhang mit privilegierten Konten erkennen und kommunizieren können. Zudem sollten sie darüber informiert werden, welche Einschränkungen bei der Verwendung dieser Konten gelten und wie sie dazu beitragen können, dass diese Einschränkungen eingehalten werden.

Ein weiterer wichtiger Aspekt der Schulung ist die Aufklärung über die Bedeutung von Compliance-Anforderungen. Mitarbeitende sollten wissen, wie PAM dazu beitragen kann, diese Anforderungen zu erfüllen und welche Konsequenzen eine Nichteinhaltung haben kann. Indem Unternehmen ihren Mitarbeitenden ein solides Verständnis für PAM vermitteln, können sie das Risiko von Sicherheitsverletzungen reduzieren und ihre IT-Sicherheit insgesamt verbessern.

5. Bewertung von PAM-Lösungen

Um sicherzustellen, dass Sie die beste PAM-Lösung für Ihr Unternehmen auswählen, sollten Sie sorgfältig evaluieren und die verschiedenen Anbieter vergleichen.

Erfahren Sie mehr über die Bewertung von PAM-Lösungen und wie Sie die richtige Entscheidung treffen können, indem Sie weiterlesen!

5.1 Evaluierungskriterien

Bei der Evaluierung von PAM-Lösungen gibt es einige wichtige Kriterien, die berücksichtigt werden sollten. Zunächst sollte man darauf achten, dass die Lösung verschiedene Arten von privilegierten Accounts abdecken kann, einschliesslich lokaler Konten, Active Directory-Konten und Cloud-Konten. Eine benutzerfreundliche Oberfläche und Integration mit anderen Systemen sind ebenfalls wichtige Faktoren bei der Auswahl einer PAM-Lösung.

Ein weiteres Evaluierungskriterium ist die Fähigkeit zur Überwachung und Auditierung von privilegierten Zugriffen. Eine gute PAM-Lösung sollte in der Lage sein, Ereignisse in Echtzeit zu überwachen und detaillierte Berichte über Aktivitäten von privilegierten Benutzern zu erstellen. Eine Entitätsverhaltensanalyse ermöglicht es auch, mögliche Bedrohungen frühzeitig zu erkennen und zu verhindern.

Schliesslich sollte die PAM-Lösung einheitliche Sicherheitsrichtlinien unterstützen und Automatisierungsprozesse anbieten. Damit können IT-Verantwortliche die Zugriffsrechte von Benutzern einfach verwalten und gleichzeitig sicherstellen, dass Compliance-Anforderungen eingehalten werden. Mit einer guten PAM-Lösung kann das Unternehmen seine IT-Ressourcen effizienter nutzen und sich gleichzeitig vor Cyberangriffen schützen.

5.2 Auswahl von Anbietern

Wenn es darum geht, eine geeignete PAM-Lösung für Ihr Unternehmen auszuwählen, ist es wichtig, sorgfältig zu evaluieren und zu vergleichen. Es gibt viele verschiedene Anbieter auf dem Markt und jeder hat seine eigenen Stärken und Schwächen. Beginnen Sie mit der Identifizierung Ihrer spezifischen Anforderungen und Prioritäten, um die Suche einzuschränken.

Ein wichtiger Faktor bei der Auswahl eines Anbieters ist dessen Erfahrung und Reputation im Bereich PAM-Sicherheit. Sie möchten einen Anbieter mit einer nachgewiesenen Erfolgsbilanz und einem guten Ruf für effektive Sicherheitslösungen. Auch sollten Sie einen Anbieter wählen, der in der Lage ist, nahtlos in Ihre bestehende Systeminfrastruktur zu integrieren und dabei alle erforderlichen Compliance-Anforderungen zu erfüllen.

Zum Beispiel bieten unsere präferierten Partner wie BeyondTrust, Safeguard (One Identity) oder Saviynt eine umfassende Suite von Funktionen an, einschliesslich Passwort-Management, Identitätsmanagement und Zugangssteuerung.

5.3 Implementierung und Integration mit bestehenden Systemen

Ein wichtiger Aspekt bei der Implementierung von Privileged Access Management (PAM)-Lösungen ist die Integration mit vorhandenen Systemen. Durch die Integration mit anderen Sicherheitslösungen und IT-Systemen wird sichergestellt, dass das PAM-Tool nahtlos in bestehende Prozesse integriert werden kann. Dies erleichtert nicht nur die Implementierung, sondern verbessert auch die Übersichtlichkeit und Effizienz der gesamten IT-Sicherheitsinfrastruktur.

Bei der Auswahl einer PAM-Lösung müssen IT-Verantwortliche darauf achten, dass sie eine Lösung wählen, die mit den vorhandenen Systemen kompatibel ist. Idealerweise sollte das PAM-Tool APIs (Application Programming Interfaces) unterstützen, um eine reibungslose Integration zu ermöglichen.

Ein Beispiel für eine erfolgreiche Integration ist die Verbindung von PAM-Tools mit Single-Sign-On-Tools (SSO), damit Benutzer Zugriff auf privilegierte Konten erhalten können, ohne sich jedes Mal separat anmelden zu müssen.

Es ist wichtig, dass IT-Verantwortliche und Sicherheitsverantwortliche eng zusammenarbeiten, um sicherzustellen, dass die PAM-Lösung vollständig in die vorhandene IT-Sicherheitsinfrastruktur integriert wird. Nur so kann ein nahtloser Arbeitsablauf für alle Beteiligten gewährleistet werden.

6. Herausforderungen bei der Implementierung von PAM-Lösungen

Die Implementierung von Privileged Access Management-Lösungen kann aufgrund der Komplexität, Mitarbeiterakzeptanz und des Kostenaufwands schwierig sein. Trotzdem ist es wichtig, diese Herausforderungen zu meistern und eine effektive Sicherheitslösung für Ihre IT-Ressourcen zu etablieren.

Erfahren Sie jetzt mehr über die Best Practices und Evaluierungskriterien für PAM-Lösungen!

6.1 Komplexität

Die Implementierung von Privileged Access Management-Lösungen kann aufgrund ihrer Komplexität eine Herausforderung darstellen. Dies liegt daran, dass diese Lösungen den Zugang zu sensiblen Systemen, Ressourcen und Daten regeln und überwachen müssen, während gleichzeitig die Produktivität aufrechterhalten wird. Die oft komplexen Infrastrukturen, die von Unternehmen bereitgestellt werden, können eine Integration der PAM-Lösungen erschweren. Darüber hinaus können die verschiedenen Anforderungen der Nutzergruppen und ihre unterschiedlichen Bedürfnisse hinsichtlich des Zugangs zu privilegierten Konten und der Verwaltung von Berechtigungen zu einer zusätzlichen Herausforderung für IT-Verantwortliche werden.

Beispielsweise kann es schwierig sein, die richtigen Benutzerprofile für die Zugriffsverwaltung zu erstellen oder die Passwortrichtlinien so zu gestalten, dass sie sowohl sicher als auch benutzerfreundlich sind. Daher ist es wichtig, die Implementierung sorgfältig zu planen und klare Ziele und Prioritäten zu definieren. Eine gute Zusammenarbeit zwischen IT-Verantwortlichen und Sicherheitsverantwortlichen ist ebenfalls unerlässlich, um sicherzustellen, dass die PAM-Lösung den Anforderungen des Unternehmens entspricht und korrekt implementiert wird.

6.2 Mitarbeiterakzeptanz

Einer der häufigsten Stolpersteine bei der Implementierung von Privileged Access Management-Lösungen ist die Akzeptanz der Mitarbeitenden. Viele Mitarbeitende empfinden es als unnötige Einschränkung, wenn sie plötzlich keinen uneingeschränkten Zugriff mehr auf Systeme haben. Aus diesem Grund ist es wichtig, das Bewusstsein und Verständnis der Mitarbeitenden zu schärfen.

Dazu können Schulungen und Workshops angeboten werden, um die Bedeutung von PAM Lösungen zu verdeutlichen und mögliche Bedenken auszuräumen. Es kann auch hilfreich sein, einige konkrete Beispiele von erfolgreichen Cyberangriffen zu präsentieren und die Auswirkungen auf das Unternehmen zu zeigen. Dadurch wird deutlich, dass PAM nicht nur eine lästige Einschränkung darstellt, sondern eine wichtige Schutzmassnahme ist.

Es ist ebenfalls sinnvoll, den Mitarbeitenden zu zeigen, dass PAM-Lösungen nicht bedeuten, dass sie keinen Zugriff mehr auf Systeme haben werden. Vielmehr geht es darum, privilegierte Konten nur dann zu nutzen, wenn es wirklich erforderlich ist und die Sicherheitsrisiken bei ungehemmtem Zugang zu minimieren. So können Mitarbeitende weiterhin in der Lage sein, ihre Arbeit effektiv zu erledigen, während gleichzeitig das Unternehmen gegen potenzielle Cyberangriffe geschützt wird.

6.3 Kostenaufwand

Die Implementierung von Privileged Access Management-Lösungen kann mit erheblichen Kosten verbunden sein. Der Kauf und die Integration von PAM-Software sowie die Schulung von Mitarbeitenden erfordern oft beträchtliche Investitionen. Auch die Aufrechterhaltung und Aktualisierung der Systeme können erhebliche Kosten verursachen. Darüber hinaus können die Kosten für die Bewältigung von Sicherheitsrisiken durch unzureichend geschützte Konten oder Datenlecks signifikant sein.

Trotz der möglichen Kosten ist es wichtig zu betonen, dass eine Investition in PAM-Lösungen langfristig gesehen lohnenswert sein kann. Ein erfolgreicher Angriff auf privilegierte Accounts kann zu schwerwiegenden finanziellen und rechtlichen Konsequenzen führen, einschliesslich Bussgelder oder Schadensersatzforderungen. Durch die Implementierung von PAM-Systemen können Unternehmen nicht nur ihre Systeme sicherer machen, sondern auch Sicherheitsrisiken minimieren und Compliance-Anforderungen erfüllen.

Es ist jedoch wichtig, dass Unternehmen bei der Implementierung von PAM-Lösungen sorgfältig planen und evaluieren. Eine sorgfältige Analyse des Bedarfs und gründliche Evaluierung der verfügbaren Lösungen können dazu beitragen, unnötige Kosten oder Fehler bei der Implementierung zu vermeiden.

Fazit und Ausblick

Insgesamt ist es unerlässlich, dass Unternehmen eine Privileged Access Management-Lösung implementieren, um ihre IT-Ressourcen und sensiblen Daten vor Bedrohungen zu schützen. Das Zugriffsmanagement ist ein wichtiger Bestandteil der IT-Sicherheit und benötigt eine angemessene Kontrolle, um Risiken zu minimieren. PAM-Lösungen bieten zahlreiche Funktionen wie Passwort-Management, Zugriffsmanagement und Überwachung, um die Sicherheit der Systeme zu erhöhen.

Bei der Implementierung von PAM-Lösungen sollten Best Practices berücksichtigt werden. Dazu gehören die Identifizierung privilegierter Accounts, die Implementierung von Least-Privilege-Prinzipien und die Schulung der Mitarbeitenden. Die Auswahl eines Anbieters und die Integration mit bestehenden Systemen können jedoch Herausforderungen darstellen.

In Zukunft wird die Komplexität von PAM-Produkten weiter zunehmen und es wird immer wichtiger, dass IT-Verantwortliche sich über Zugangsrechte-Management, Berechtigungsverwaltung, Sicherheitsrichtlinien und Compliance informieren und entsprechende Massnahmen ergreifen. Die Entitätsverhaltensanalyse wird eine zentrale Rolle bei der Erkennung von Bedrohungen spielen und die Verwaltung von Benutzerrechten wird noch einfacher und intuitiver werden.

Sichern Sie Ihre Daten und schützen Sie Ihr Unternehmen mit einer PAM-Lösung! Kontaktieren Sie uns noch heute, um zu erfahren, wie wir Ihnen helfen können.

Scan me

IPG AG
Theaterstrasse 17
CH-8400 Winterthur

IPG GmbH Deutschland
Hertzstrasse 20
DE-13158 Berlin

IPG Austria GmbH
Johann-Strauß-Gasse 32
AT-1040 Wien

www.ipg-group.com

info@ipg-group.com