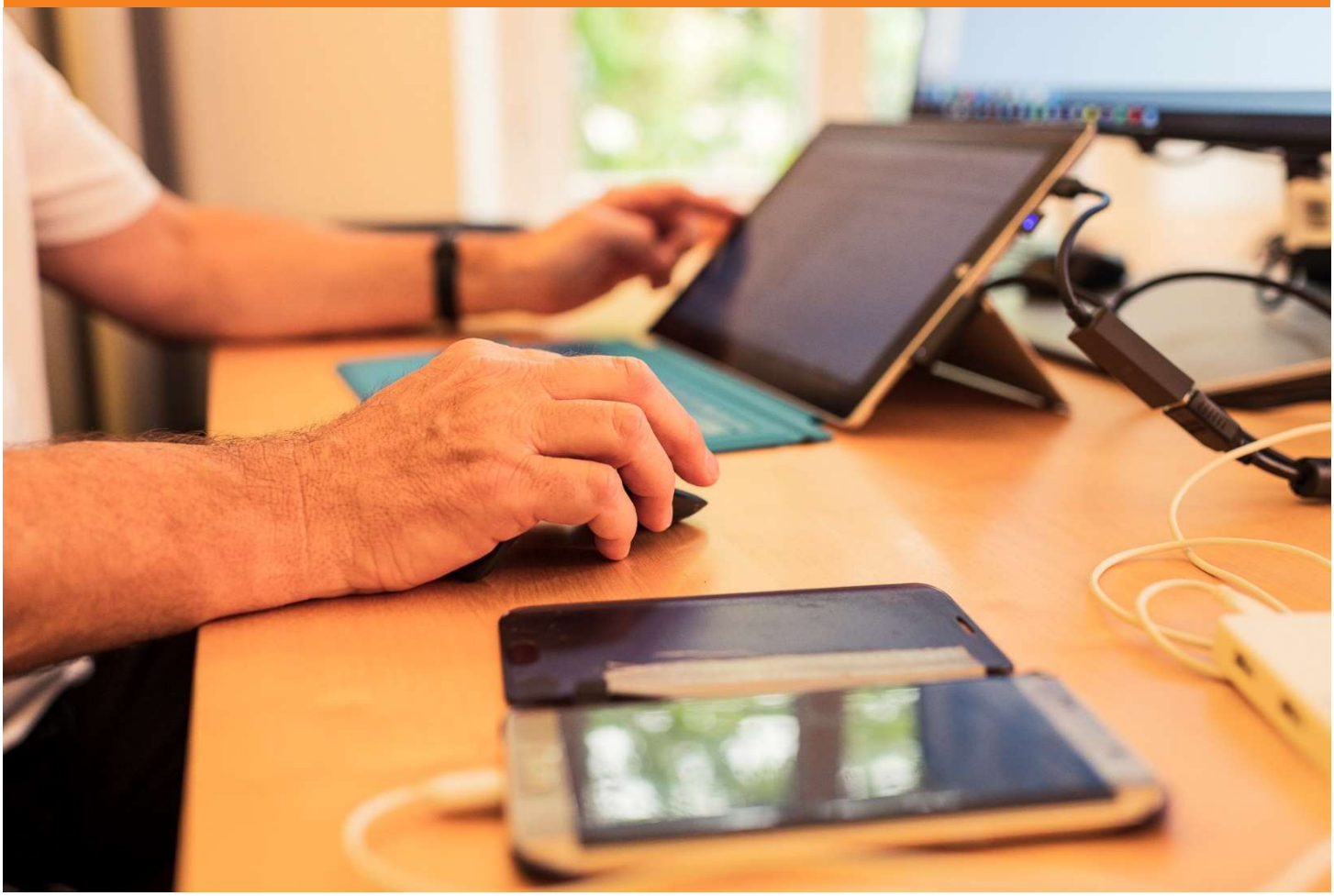
To PAM or not to PAM – That is the question

Nach Identity and Access Management (IAM) nun Privileged Access Management (PAM)

Thema Security



Privilegierte Benutzerkonten sind ein beliebtes Ziel für Attacken. Und wie bei Hamlet vor über 400 Jahren, droht die Gefahr von innen wie auch von aussen. Deshalb müssen die privilegierten Benutzerkonten mit grosser Sorgfalt verwaltet und gesichert werden.

Bereits seit einigen Jahren hat sich Identity und Access Management (IAM) nicht nur bei grossen, sondern auch bei kleineren und mittleren Unternehmen etabliert. Vor allem mit dem Ausbau von webbasierten Anwendungen, dem Aufkommen von APIs sowie dem immer grösseren Druck hin zu Cloud Lösungen wird eine gut funktionierende Benutzer- und Berechtigungsverwaltung unumgänglich. Während der Fokus bei IAM anfänglich hauptsächlich auf der Zugriffskontrolle für die (End-)Benutzer einer Organisation lag, rücken nun vermehrt die privilegierten Benutzerkonten ins Zentrum der Betrachtung.

Eine wichtige Eigenschaft von privilegierten Benutzerkonten besteht darin, dass man deren Zugriffe zu bestimmten Systemen nicht einschränken kann oder es unter Umständen nicht möglich ist, einen personalisierten Zugriff zu erstellen. Als Beispiele:

- Ein Datenbankadministrator benötigt hohe Rechte, um seine Arbeit effizient erledigen zu können
- Ganz ohne Root Account wird es im Linux Umfeld schwierig
- In der Social Media Abteilung arbeiten gegebenenfalls mehrere Leute mit demselben Twitter Account

Der Fokus einer PAM-Lösung liegt auf der nachvollziehbaren Verwendung solcher privilegierter Konten unter striktem Einhalten des sogenannten Least Privilege-Prinzips, sprich dem Prinzip, dass ein Benutzerkonto jeweils möglichst nur die notwendigen Rechte verfügen soll.

Ein solides Framework für PAM

Um alle zu behandelnden Themenfelder rund um PAM abzudecken, empfiehlt es sich ein etabliertes Framework zu verwenden. Ein solches Framework stellt das Capability Framework für Privileged Access Management der ISACA [1] dar. Das Capability Framework für PAM der ISACA unterteilt PAM-Lösungen in vier Domänen, welche ihrerseits jeweils verschiedene Bereiche des PAM abdecken.

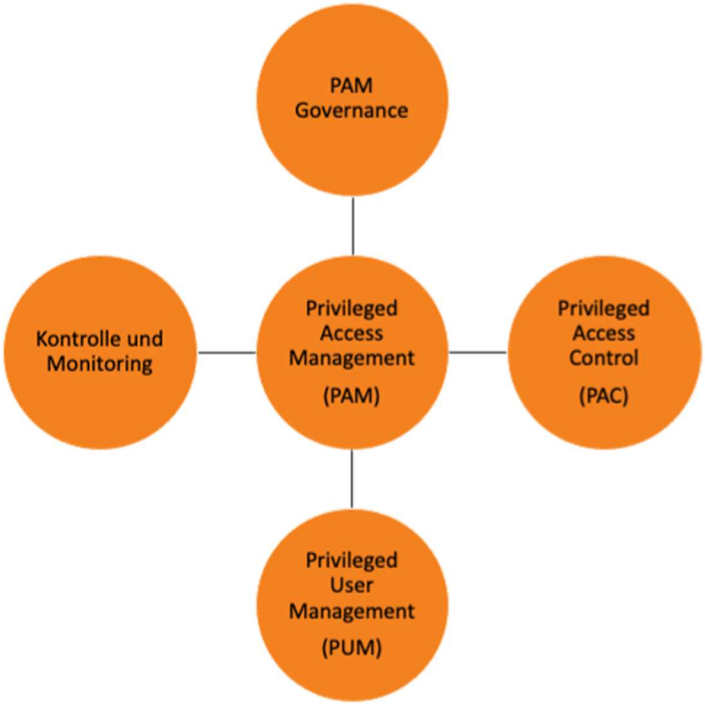


Abbildung 1: Die Domänen des Capability Framework für Privileged Access Management der ISACA

PAM Governance

Ad Hoc-Lösungen und unstrukturiertes Vorgehen im Bereich PAM erschweren es den gewünschten Schutz von privilegierten Benutzerkonten sicherzustellen. Mit klaren Governance-Vorgaben kann der Rahmen für eine umfassende und ganzheitliche PAM-Lösung geschaffen werden. Ziel dieser Governance-Vorgaben ist, dass involvierte Stellen und Personen die Notwendigkeit der PAM-Lösung nicht nur verstehen, sondern auch unterstützen.

Inventar der Zugriffswege für privilegierte Zugänge

Solange man nicht genau weiss, welche Zugangswege für privilegierte Benutzerkonten in der eigenen Organisation bestehen, kann man diese nicht adäquat schützen. Es gilt daher sicherzustellen, dass die Arten von Zugangswegen für privilegierte Zugänge bekannt sind und das Vorgehen bestimmt ist, neue Zugangswege zu verwalten.

Umgang mit privilegierten Benutzern

Ob missbräuchlich oder nicht, der Missbrauch der privilegierten Benutzerkonten kann schwerwiegende Folgen haben. Es ist darum notwendig, klar definierte Prozesse für die Vergabe, Überprüfung und den Entzug von Rechten zu definieren und umzusetzen. Hinzu kommen Compliance-Anforderungen für die Nachvollziehbarkeit der Vergabe sowie die Nutzung der privilegierten Benutzerkonten.

Controlling und Monitoring

Neben dem klassischen Aufzeichnen der Zugriffe ist das gesamte Session Recording ein Thema im Bereich der Überwachung der Zugriffe. Zusammen mit einer SIEM-Lösung können im Idealfall nahezu in Echtzeit Manipulationen überwacht werden und Gegenmassnahmen eingeleitet werden.

Vorgehen zur Umsetzung des Frameworks

Mit Hilfe des Capability Frameworks lassen sich auf sehr einfache Weise die Ziele für eine PAM-Lösung definieren. Diese Ziele dienen wiederum dazu, den Grundstein für eine sichere Verwaltung der privilegierten Zugänge zu legen.

Eine GAP Analyse erlaubt es die Defizite in der aktuellen PAM Umgebung zu identifizieren, die notwendigen Schritte zu definieren und auf Grund einer Risikoeinschätzung zu priorisieren.

Damit Spezialfälle und Eigenheiten der bestehenden Infrastruktur und Prozesse mit einfliessen, bieten sich neben der Sichtung und Auswertung bestehender Dokumente vor allem Interviews mit den Stakeholder an. Im Rahmen dieser Interviews werden zudem nicht nur GAPs identifiziert, sondern auch das Bewusstsein für einen sicheren Umgang mit den privilegierten Zugängen gestärkt.

Je nach Umfang der identifizierten GAPs und den vorgeschlagenen Massnahmen lassen sich Arbeitspakete definieren, Projektinitiativen starten oder Quick Wins identifizieren. Eine Kosten-Nutzen-Analyse hilft hier zusätzlich, die vorhandenen Ressourcen effizient und zielgerichtet einzusetzen.

Mit unserer Erfahrung im Bereich des Privileged Access Management stehen wir als Partner gerne bereit, um mit Ihnen zusammen den Umgang mit Ihren privilegierten Benutzern und Zugängen sicher zu gestalten. So können Sie sicher sein, dass es Ihrem Unternehmen nicht so ergeht wie Hamlet und seinem Königreich.

The Readiness Is All. - William Shakespeare, Hamlet

[1] https://www.isaca.org/resources/isaca-journal/issues/2017/volume-1/capability-framework-for-privileged-access-management