افزایش تهدیدات امنیتی پیچیده و هدفمند توسط مهاجمان خارجی و خودی های مخرب ، محافظت صحیح از اطلاعات مهم و حساس را برای سازمان ها بسیار دشوار کرده است. وظیفه حفاظت از این دارایی ها به مراتب سخت تر شده است چرا که محیط های فناوری اطلاعات پیچیده تر شده و به طور گسترده در نقاط جغرافیایی و ابر توزیع شده اند.

متجاوزان حساب های ممتاز را به سرقت برده و از زیرساخت های کل شرکت سو استفاده کرده اند. متأسفانه ، بسیاری از مدیران فناوری اطلاعات درک کاملی از نحوه عملکرد حسابهای ممتاز و همچنین خطرات مرتبط با سازش و سو استفاده از آنها ندارند. این امر باعث می شود که آنها و سازمان هایشان در برابر آسیب های احتمالی پولی و اعتباری بسیار آسیب پذیرتر باشند. مدیریت دسترسی ممتاز Previldge Access Management-PAMراهکاری برای مقابله با این مسئله است.

شرکت رایان سامانه آرکا، نماینده رسمی سنهاسگورا Senhasegura و Arcon در ایران است که هر دو جزو PAM های مطرح و جامع بازار است.

ویژگیها و امکانات:

- مدیریت و کنترل سطوح دسترسی کاربران ارشد، برنامه ها و سیستم های عمل
- جلوگیری از اعمال سهوی یا عمدی دستورات مخرب با دسترسی سطح بالا بر روی سیستم های حیاتی
- مدیریت دسترسی برای کاربران از راه دور

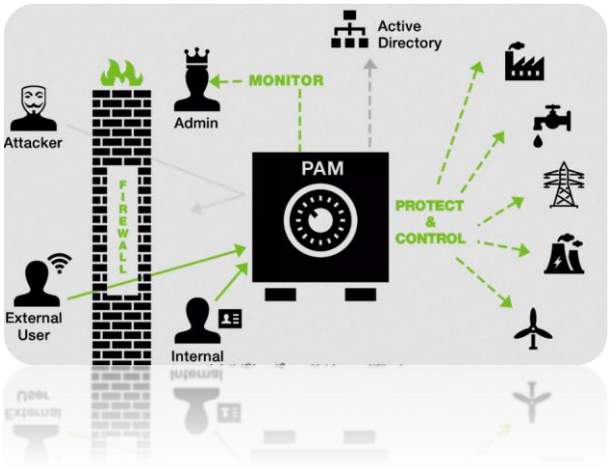
PAM به چه شکلی کار میکند؟

PAMمابین منابع سازمان (سخت افزار ها، نرم افزار، روتر و سویچ ها، سیستم کاربران عادی و...) و کاربران ادمین قرار می گیرد. سپس منابع روی سرور PAM تعریف می شود یعنی آدرس ها، یوزر اکانت ها و پسورد منابع در پنل PAM ثبت می شود. سپس نسبت به سیاست های سازمان تعیین می کنیم که چه ادمینی به چه منابعی دسترسی داشته باشد.
سپس کافیست تا ادمین از طریق کنسول وب به PAM لاگین کرده و دستگاه هایی که مجاز به دسترسی به آن ها می باشد را ببیند و بدون نیاز به وارد کردن پسورد دستگاه مقصد به آن دستگاه متصل شده و کار های خود را انجام دهد. ضمن آنکه در این حالت تمام رفتار های ادمین قابل کنترل و مانیتور می باشد.
در این حالت اگر اتفاق غیر قابل پیش بینی رخ دهد کاملا قابل پیگیری خواهد بود. همچنین فیلم رکورد شده تغییرات انجام شده در سیستم PAMذخیره میشود. و قابل مشاهده توسط ادمین PAM می باشد.
همجنین در سیستم PAM قابلیت و فیچر های دیگری همچون محدود کردن اجرای یک دستور خاص در SSH و Telnet وجود دارد. از دیگر قابلیت های PAM می توان به محدود کردن اجرای یک برنامه توسط ادمین در سیستم کاربران و سرور ها می باشد.

PAM درباره

امروزه مدیران ارشد سازمان ها برای بالا بردن سطح امنیت و حفاظت از دارایی های اطلاعاتی خود سرمایه گذاری ویژه ای میکنند. و از محصولات و راه کار های متنوعی بهره می برند. برای مثال: درگاه های شبکه را به انواع دیوار های آتش، IPS، WAF، UTMو ... مجهز می کنند. حتی از روش ها و استاندارد های امنیتی، مانند PCI-DSS :و ISO27001 بهره می گیرند. اما در نهایت برای اینکه کار سازمان به انجام برسد به ناچار مجبور هستند دسترسی های سطح بالا، به سامانه های اطلاعاتی، نرم افزارها، سخت افزار ها و سرور های سازمان را به پیمانکار و یا افرادی بسپارند. شایداین افراد به صورت تمام و کمال مورد اطمینان و وثوق شان نباشند. آمار ها نشان می دهند که در سازمان های بزرگ، ریسک ها و تاثیر آسیب هایی که این افراد به مجموعه وارد می کنند بسیار قابل تامل است.

فارغ از اینکه علت و انگیزه چه میتواند باشد و یا اینکه حوادث رخ داده عمدی بوده اند یا سهوی، نتیجه و تاثیر بسیاری از وقایع غیرقابل جبران است



بنابراین راهکاری باید اتخاذ گردد که بتواند این ریسک را پوشش داده تا چشم بسته به افراد اعتماد نکرده و منابع سازمان را بتوانیم با خیال آسوده در اختیار این کاربران قرار دهیم. این راهکار با نام اختصاری PAM به معنی privilege Access Manager شناخته میشود. در دنیا فقط چندین محصول قدرتمند وجود دارند. که این ریسک و نیاز را برای ما فراهم میکنند. از جملهCyberArk , WALLIX, Senhasegura و محصولات دیگری که در این زمینه فعال می باشند.