PRIVILEGED ACCOUNT MANAGEMENT (PAM)

BOB LANNOY

1. Inleiding

De laatste jaren duiken steeds meer verhalen op in de pers van bedrijven waar al dan niet bewust gegevens verloren zijn gegaan of systemen gesaboteerd werden. Ondanks dat deze verhalen sterk gemediatiseerd worden door security vendors zit er een grond van waarheid in. Heel wat gebruikers beschikken buiten hun standaardrechten op systemen soms ook over meer geprivilegieerde rechten, zoals nodig voor administratiedoeleinden. De fractie aan “insider”-veiligheidsincidenten is laag in vergelijking met veiligheidsproblemen van buitenaf maar hun impact is des te groter. Dit gaat van imagoschade tot serviceonderbrekingen.

Elk systeem heeft wel een administratieaccount zoals *Administrator* (Windows), *root* (Unix), SYS (Oracle), ... In tegenstelling tot normale gebruikersaccounts zijn deze niet gekoppeld aan een persoon maar kunnen die gedeeld worden met mensen die het wachtwoord kennen van deze accounts. Het wachtwoord van gedeelde accounts wordt niet snel gewijzigd en soms onvoldoende beschermd. Als een account werd gebruikt weet men niet wie de fysieke persoon achter het toetsenbord was.

Privileged Account Management (kortweg PAM) heeft tot doel de geprivilegieerde toegang tot systemen te regelen en te controleren en maakt deel uit van het arsenaal aan tools beschikbaar voor security governance.

2. Aanpak en functionaliteit

PAM is echter niet beperkt tot systeemaccounts maar omvat ook accounts die toepassingen gebruiken om met een database te communiceren of toepassingen met elkaar te laten communiceren. Vaak worden de wachtwoorden van deze accounts opgeslagen in een configuratiebestand of in de code al dan niet beveiligd met behulp van encryptie.

Veel PAM-tools bieden de mogelijkheid om standaardgebruikers tijdelijk administratietaken te laten uitvoeren via “privilege elevation”. Een klassiek voorbeeld is *sudo* uit de Unix-wereld.

Tenslotte is er de mogelijkheid om sessies op te nemen en doorzoekbaar te maken, als ook de generatie van allerlei rapporten die audit-activiteiten ondersteunen.

Het begrip PAM mag niet vernauwd worden tot het gebruik van een tool. Men kan vertrekken vanuit een aantal security best-practices en processen gesteund op technologische keuzes, zoals:

- Ken uw (nieuw) personeel, zijn er bijvoorbeeld mensen die een risico kunnen vormen?
- Opleidingen: maak mensen bewust van risico's, vaak zijn mensen er zich niet van bewust dat ze risicogedrag vertonen.
- *Segregation-of-duties*: combinatie van taken geeft aanleiding tot risico, het scheiden van die taken moet dit verhinderen.
- Monitoring/logging naar extern systeem beheerd door andere personen, hierdoor verlaagt de kans dat een hacker de logs manipuleert.
- Systeemadministrators hebben een eigen account voor beheertaken in plaats van een gedeelde account, waar mogelijk. Dit maakt het makkelijker om de link met de fysieke persoon te maken.

Specifiek voor geprivilegieerde accounts kan je een aantal gradaties onderscheiden in aanpak, van de meest eenvoudige basismaatregelen tot de inzet van een specifieke tool:

- Elk systeem heeft een eigen (voldoende complex) wachtwoord, en niet bijvoorbeeld op alle servers hetzelfde administratie-wachtwoord.
- De administratiewachtwoorden worden bijgehouden in een beschermde omgeving met gecontroleerde toegang tot de wachtwoorden.
- Er is een policy om op regelmatige basis de wachtwoorden (van de meest kritische systemen) te wijzigen.
- Bepaalde tools en scripts worden toegepast om gebruikers tijdelijk hogere rechten te geven, zoals *sudo* (Unix) zodat ze het administratiewachtwoord niet hoeven te kennen.
- Het inzetten van PAM-software als een silo in een organisatie of voor specifieke systemen.
- Een geïntegreerde aanpak waar PAM wordt gebruikt in combinatie met andere security-technologie.

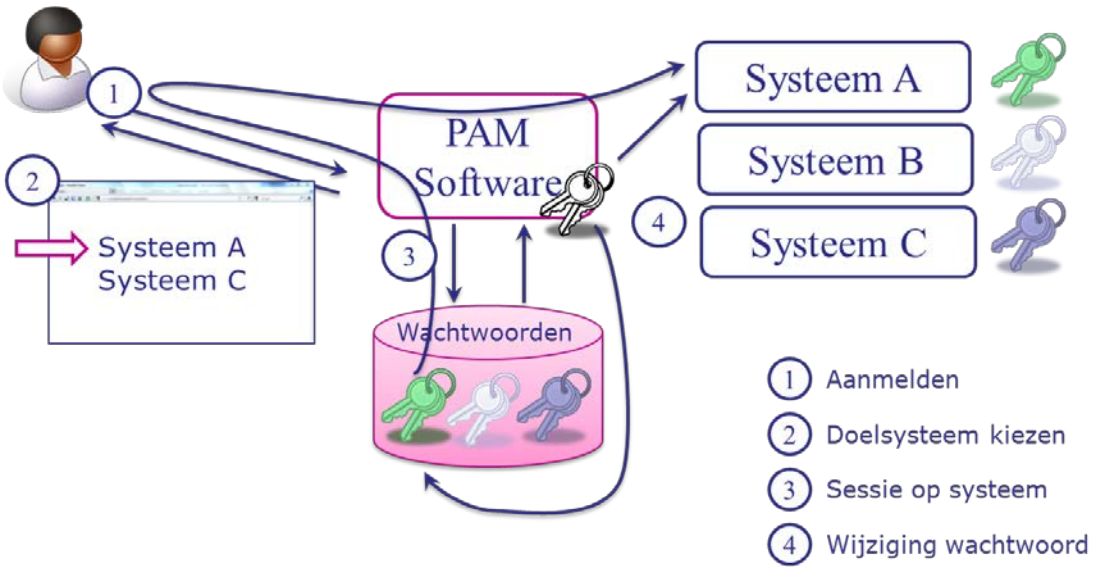
3. Geïntegreerde tools

3.1. Leveranciers & werking

Er zijn een aantal softwareleveranciers van PAM-oplossingen zoals BeyondTrust, CA, Cyber-Ark, Lieberman Software en Quest (nu Dell).

Een centrale databank slaat alle wachtwoorden op en heeft via connectoren (SSH, HTTPS, WMI, ...) toegang tot de beheerde systemen. De tool zal op die systemen op vastgestelde events het wachtwoord van de account wijzigen en controleren.

Het gebruik wordt schematisch weergegeven in Figuur 1. Een gebruiker meldt zich aan via een web-interface (1) om toegang te krijgen tot een account (2). Na de nodige autorisatiecontroles, al dan niet ondersteund door een goedkeuringsworkflow, krijgt de gebruiker het wachtwoord te zien of onmiddellijk een sessie zonder het wachtwoord ooit te zien te krijgen (3). Het PAM-systeem kan het wachtwoord ook nog wijzigen na gebruik (4).



Figuur 1: Werkingsprincipe

Het platform beschikt over heel wat middelen om een audit mogelijk te maken, zoals logging en rapportering van alle activiteit maar ook het opnemen van de uitgevoerde sessies en het consulteerbaar maken.

De prijsmodellen van leveranciers verschillen sterk van elkaar. Er zijn heel wat parameters die kunnen meespelen: de gewenste functionaliteit (wachtwoorden beheren, applicatieaccounts, sessies opnemen), aantal te beheren servers, aantal gebruikers, aantal concurrent sessies, ...

3.2. Prototype

In het kader van de studie werd een testomgeving opgezet met Windows en Linuxservers, een Oracle databank, een WebLogic applicatieserver en netwerkapparatuur. Met behulp van een PAM-tool werd de integratie met de diverse systemen uitgetest.

Dit prototype gaf een goed beeld van de functionaliteit van de tool en de impact van dergelijke tool op een omgeving. De implementatie gaat redelijk vlot voor standaardsystemen. Er zijn heel wat connectoren waarbij via scripting de integratie beter kan afgestemd worden. De

netwerktopologie (zoals gescheiden netwerken en DMZ's) hebben een sterke impact op de implementatie, zowel in functionaliteit als in kostprijs.

Een serverpark is geen statisch gegeven en daarom moet bij een PAM-project de nodige processen en integratie voorzien worden.

Bij het gelijktijdig gebruik van gedeelde accounts is het moeilijk te scheiden wie wat heeft gedaan tenzij er gebruik gemaakt wordt van *session recording*.

De integratie van applicaties in de PAM-tool verhoogt de complexiteit bij deployment van die applicaties. Er moet o.a. rekening gehouden worden met de authenticatie van de applicaties zelf en de wachtwoordcaches die synchroon moeten lopen met de veranderingscyclus van de wachtwoorden.

Elk team verantwoordelijk voor een stuk van de infrastructuur (Windows, Unix, DB, Middleware, netwerk, development, …) heeft een eigen aanpak voor (geprivilegieerde) accounts, met gradaties in maturiteit. Overstappen naar een PAM-tool is een ingrijpende wijziging en moet als een volwaardig project doorgevoerd worden.

4. Besluit

Het mag duidelijk zijn dat men zich bewust moet zijn van de risico's en het beheer van privileged accounts in handen moet nemen. Privileged account management vormt echter een deel van een groter geheel van Identity/Access Management, monitoring en andere security technologie. Men mag er niet van uitgaan dat door PAM te deployen men alle problemen heeft opgelost.

PAM is geen (één) tool-oplossing maar een verzameling van security best-practices en technische oplossingen. Zonder tool kan men al een aantal maatregelen nemen zoals verschillende wachtwoorden per systeem, voldoende logging, beveiligde wachtwoordlijsten, ...

Een geïntegreerde PAM-tool minimaliseert het risico van gedeelde accounts tot de beheerder van de tool. Er dient de nodige aandacht te gaan naar de gewenste functionaliteit en de doelsystemen waarmee men wenst te integreren. Een aantal aandachtspunten zijn de verhoging van complexiteit van de IT-omgeving, de impact van de topologie en IT-architectuur op prijs en functionaliteit en de gebruiksvriendelijkheid van de oplossing.

Als eindconclusie kunnen we stellen dat de keuze voor een tool afhangt de mate van het risico dat men wenst te beperken ten opzichte van de kost van een dergelijke implementatie.

Sectie Onderzoek van Smals brengt met regelmaat verschillende publicaties uit over een hele waaier aan topics in de huidige IT-markt. U kan deze publicaties opvragen via het extranet :

http://documentatie.smals.be

Of u kan rechtstreeks contact opnemen met het secretariaat van de afdeling 'Klanten & Diensten', op het nummer 02/787 58 88.