

Gestão de Privilégio e Acesso



Conceitos e Melhores Práticas

Sumário Executivo

Devido ao fato de usuários e administradores (identidades) manterem elevadas permissões de acesso aos dados para executar programas e alterar as configurações de hardware e de, praticamente, todos os componentes de software de TI, o controle sobre seu uso é essencial para manter a segurança da informação e eficiência operacional.

Apesar dos sucessos contínuos de avaliação de auditoria já realizados, de fato, existe um GAP que as organizações não conseguem controlar adequadamente o uso de identidades de privilégio elevado e acabam encontrando problemas como perda de dados, inatividade operacional e até danos à reputação.

Introdução

Identidades de privilégio elevado são contas que possuem permissão elevada para acessar sistemas. Elas existem praticamente em todos os lugares em TI como, servidores e sistemas operacionais, desktop, dispositivos de rede, roteadores, switches e dispositivos de segurança, programas e serviços, de banco de dados, aplicações de negócio, serviços web, backup, job scheduling e outros sistemas.

Assim, novos jargões como: *SAPM*, *PUPM*, *PPM* aparecem no mercado para resolver este problema de contas de privilégio elevado, que são respectivamente: *Service\Share Account Password Management*, *Privilege User and Password Manager*, *Privilege Password Management*.

É justamente por este motivo que, por considerar usuários (identidades) de privilégio elevado, o seu gerenciamento deveria ser tratado com maior atenção dentro das empresas. Para detalhar o assunto e atenção requerida, devemos iniciar com a definição de usuários (identidades) de uma empresa comum. Normalmente existem 3 tipos de usuários de domínio nas empresas:

- **End-User** (Usuários Normais ou Padrões), com Uso Individual, com pouco acesso e com informações restritas, e privilégios restritos;
- **Admin** (Administradores ou SuperUsers), com uso compartilhado, existente para realizar mudanças de configuração (planejadas ou não) e que possui acesso elevado a informações, e privilégios elevados. Exemplos de Contas SuperUsers: Administrator, Local Admin, Root, IBMUSER, as, db2admin, sysadmin, mqm, admin CISCOIOS e JUNOS;
- **Application** (Contas de Serviço), com o uso compartilhado, e dependente de uma aplicação específica, que necessitam de privilégio elevado para desempenhar sua tarefa (Aplicações – A2A, Banco de Dados – A2DB, Monitoração de Desempenho, Backup entre outros), e privilégios elevados.

Projetos de Identidade (IdM) focam apenas o privilégio de acesso e restrito das contas de usuário normais e padrões incluindo, provisionamento (criação, movimentação e exclusão) e *Sign On / Autenticação* (entrada e login automático) do usuário na rede interna, mas são falhos ou inexistentes para tratar usuários (identidades) do tipo *Admin ou Application*.

E porque isto é um problema a parte e qual o tamanho e consequência de negligenciar este ponto? Considerando um exemplo real de uma empresa do setor bancário, cliente da LiebSoft, para cada pessoa do perfil administrador de TI (Admin, Root, sa, sysadmin, iosadim) existem até 1.000 contas com privilégio elevado, sendo que 20% deste valor são atribuídas a pessoas humanas e 80% a aplicações.

Estes valores podem parecer fora de propósito, mas vendo os fatos no dia-a-dia, percebemos uma falta de controle de acesso a contas de privilégio elevado no decorrer do tempo, por vários motivos:

- Criação constante de contas de serviço que são geradas para implantações de novos servidores, *appliances*, sistemas de *backup* e software controle, administração e monitoração;
- Novas aplicações são instaladas com novos *logins* internos (e muitas vezes, não são documentados por esquecimento);
- *Sobreposição* de funções de grupos de trabalho para um projeto multidisciplinar;

- *Outsourcing* ou contratação externa da administração de servidores ou processos de *hosting, collocation* e até mesmo *amazonation (cloud computing)*;
- Falta de controle em gestão de identidade, que é provisionamento (criação\remoção) de usuários administradores.

Por isto, parte crucial deste trabalho é fazer um diagnóstico situacional/levantamento (Discovery) destas contas. Isto quer dizer, achar todas as contas que constam dentro das empresas.

Depois do levantamento, o próximo desafio será efetivar as boas práticas de governança e GRC recomendadas como a troca de senhas, no mínimo, a cada 3 meses (o ideal seria mensalmente). Mas, também, é uma atividade humanamente impossível, por 2 motivos: o volume destas contas e as implicações desconhecidas que isto acarretaria, incluindo a parada de sistemas.

A prática real de mercado está longe de ser um *“best practices”*, pois, além de ser deficiente, abre um espaço para espionagem e fraudes internas, sem contar o trabalho manual de execução: cofres, cerimônias, senhas divididas e muitas vezes, até associar a uma pessoa, uma senha, para acessar uma multiplicidade de sistemas de alto valor, que constitui um risco adicional.

Mas, não ache que este é apenas um problema para empresas brasileiras, na verdade é uma realidade mundial, gerando um GAP de vulnerabilidade e segurança, devido a falta de atenção maior na gestão de senhas. Não é à toa, que o Gartner prevê que até 2010 cerca de 50% dos grandes bancos mundiais adotarão uma solução de política de senhas/privilégios ou SAPM.

A melhor estratégia, ou *“best practices”*, seria associar uma senha diferente para cada sistema, como se existisse uma varinha mágica para garantir que os administradores “lembrassem” (sem anotar e com dupla custódia) de todas elas. Lógico, é impossível sem o envolvimento de tecnologia. Além do mais, pobres dos Administradores que por diversas vezes realizam mágicas no Datacenter e não mereceriam tal atribuição.

A Solução é controlar e automatizar todas as senhas através de um sistema central e consolidado, onde as senhas são geradas e propagadas para os sistemas remotos (destino). Assim essas senhas não são compartilhadas a todo o momento, e somente à medida que se faz necessário alguma intervenção (planejada ou não). Para isto, existe um processo de workflow, solicitação, aprovação e liberação do gestor responsável (pode ser definido por tempo ou perfil). Uma vez que a senha fosse gerada e usada pelo administrador, ela seria automaticamente descartada e uma nova senha gerada (que não será compartilhada, até outra demanda solicitada). Tornando um método Seguro e Auditável.

A grande questão é que estas intervenções (planejadas ou não, documentadas ou não), não escolhem hora, lugar e dispositivo, o que acarreta outro tipo de gestão denominada *“Firecall”*.

Firecalls

Firecall (chamada ou alerta de fogo) poderia ser traduzido como o método criado para fornecer acesso de emergência a um sistema de informação.

No caso de algum um erro crítico, os usuários não privilegiados podem ter acesso aos sistemas para corrigir o problema. Quando um *firecall* é usado, normalmente há um processo de revisão para garantir que o acesso foi devidamente utilizado.

No *Mainframe\RACF* existe um tratamento simples e eficiente onde uma organização pode definir uma conta de *firecall*, para algumas aplicações específicas, mesmo com um perfil de OPERADOR. Como este modelo não pode ser aplicado a outras plataformas (distribuídas) é necessário que as senhas de acesso a *firecalls* sejam armazenadas de forma segura e sejam acessadas de forma rápida, pois qualquer demora significa indisponibilidade e impacto no negócio (Segurança x Disponibilidade).

A Natureza de contas *firecalls* é temporal, isto é, são disponibilizadas apenas por um tempo suficiente para execução da intervenção. Após isto, uma nova senha deve ser gerada para esta conta.

Normalmente, todos estes processos são manuais, isto é, a senha é escrita em algum caderno ou envelope e liberada sob solicitação e algumas vezes até duplo controle\custódia: 2 envelopes, 2 cadernos, 2 ou mais pessoas, tornando o processo: incômodo, lento e até embaçado.

Contas Compartilhadas

Outro ponto de atenção refere-se a “senhas de administrador compartilhadas”. Como o nome diz, são contas compartilhadas por um ou mais usuários. Estas contas são diferentes de contas de usuário que podem ser associado a uma determinada pessoa. A política e prática de mercado dizem que contas associadas a um determinado usuário " não deveriam ser compartilhadas", já que invalida a segurança e a auditoria aplicadas a essas contas de acesso (individualização /responsabilização). Isso seria o ideal, porém nem sempre possível.

Existem dois principais riscos de segurança com qualquer tipo de conta compartilhada.

O primeiro é que com o acesso de várias pessoas da mesma conta, é impossível manter a trilha de auditoria, pois existem vários *logins* de uma conta ao mesmo tempo. Há também a responsabilidade (*accountability*) mínima do uso da conta, e como é compartilhada, muitas vezes as pessoas não se sentem responsáveis pela segurança e fazem coisas que não fariam com o seu próprio usuário, como escrever em algum *post-it*.

O segundo risco de gestão é a senha. Imagine mudar uma senha compartilhada por muitos. Isso requer que a senha seja distribuída de uma maneira segura. Isto pode significar mais trabalho, e propensão a erros e possíveis falhas no tratamento destes.

O fato é que:

- Contas de Administrador (superusers) possuem acesso ilimitado;

- Situação de Manutenção, ou Firecalls, normalmente ocorrem após o horário normal de trabalho, e são lidadas de forma frágil;
- Existe uma falta de controle.

Best Practices

Entre as melhores práticas no controle de privilégios podemos entender que, de um lado, há grande necessidade de prevenir uso de contas compartilhadas e na responsabilização individual. Ambas são exigidas por normas regulatórias de mercado, porém, de outro lado, existe a necessidade de garantir a disponibilidade e continuidade dos negócios (que exigem o uso destes privilégios elevados para intervenções e aplicações).

Assim, a primeira ação é criar um processo para suportar este paradigma, que constitui de 6 passos: **1) Solicitação, 2) Aprovação, 3) Obtenção 4) Uso, 5) Fechamento e Bloqueio, 6) Trilha das atividades e Auditoria.**

Importante frisar que, devido à necessidade e agilidade das intervenções sem uma automação destas etapas, o processo fica fraco e dependente de pessoas e fatores extras e subjetivos, inclua aqui: importância e cargo do solicitante, análise do gestor, prioridade e cronograma do projeto em questão, e não menos importante, a confiança e amizade entre as partes.

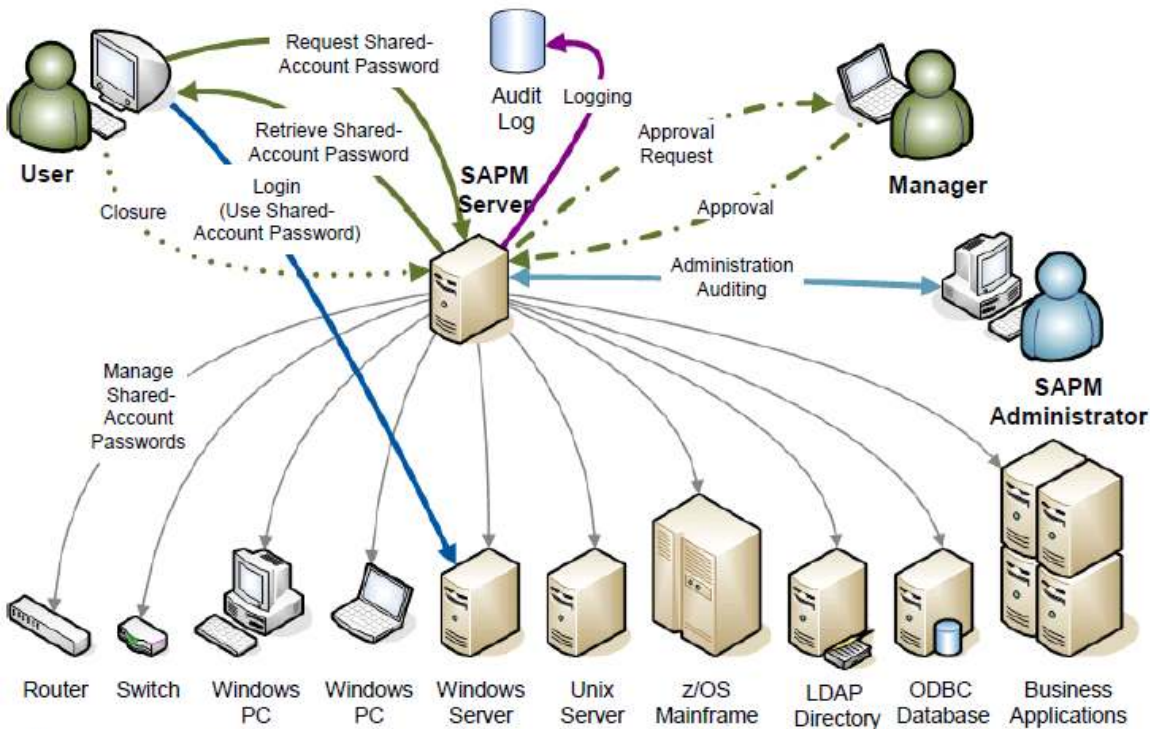
Outras ações recomendadas são:

- Minimizar o número de contas compartilhadas usados rotineiramente. Restringir o uso compartilhado de contas "superuser" para circunstâncias especiais. Se necessário "superuser" no dia-a-dia de operações normais, recomenda-se não compartilhar senhas e automatizar o processo.
- Definir uma política para contas de serviço de aplicações de monitoração, backup e outros, que inclua mapeamento por missão crítica, unidade de negócios ou geografia entre os outros divisores. Não é recomendado atribuir uma única conta para inúmeros sistemas (atenuação da política) nem, tão pouco, uma conta por dispositivo (*overhead* de trabalho).
- Utilização de ferramentas de gestão de eventos para controlar, correlacionar e analisar atividade da conta em todos os sistemas.
- Estabelecer processos e controles para a gestão compartilhada de suas senhas, mas esteja ciente de que os processos manuais e controles não são escaláveis e necessitam de cuidado e supervisão. Implante a ferramenta de gerenciamento de senha ou similar para automatizar processos, impor controles e fornecer uma trilha de auditoria.

Justamente pelo último item, empresas oferecem soluções que automatizam este processo frágil, algumas, no mercado desde 1978 (caso da LiebSoft). Estas soluções, na verdade, encapsulam todas estas etapas em envelopes de senhas de forma segura e flexível, pois, oferecem uma interface amigável para solicitação e aprovação/liberação de acesso (senha). Permitem, ainda, que

o usuário solicite conforme o perfil e política de acesso. Por último, disponibiliza senhas de acesso sem que haja intervenção humana (principalmente do administrador de redes), com as trilhas de auditoria e de forma temporal, apenas para a intervenção solicitada.

Notional SAPM Architecture and Workflow



Source: Gartner (March 2008)

Questões:

Por fim, apresentamos questões para serem refletidas e que ajudam no processo situacional de gestão de senhas, incluindo convencimento interno e ponto de atenção do assunto:

1. Precisamos fazer reparos de emergência

- Quantas vezes você precisa de acesso de administração ou de "super usuário" para executar tarefas?
- Qual o tempo gasto para conseguir estas senhas?
- Existe algum sistema ou aplicativo que você precisa de autorização especial para acessá-lo e realizar suas tarefas?
- Quanto tempo leva para ter o acesso a este sistema/aplicativo?
- Você conhece todos os sistemas/aplicativos na rede que você pode precisar de acesso para fazer seu trabalho?
- Qual o impacto de acessar um sistema com urgência, e não conseguir permissão para acessá-lo?

2. Implantação de novos sistemas e aplicações

- a) Quando foi o último grande “rollout” de hardware ou software? Quantos sistemas/aplicativos foram envolvidos?
- b) Existe uma política para mudar a configuração default de contas privilegiadas sobre esses sistemas/aplicativos?
- c) Quanto tempo leva para mudar este procedimento/configuração?
- d) Você se sente confiante que sua equipe é capaz de fechar todas as potencialidades falhas de segurança a cada nova implantação de sistemas?
- e) Existe a preocupação de deixar as vulnerabilidades de segurança?
- f) Como é que funciona a documentação de contas privilegiadas que são introduzidas com o novo hardware e software? Este é um processo manual? Leva muito tempo?

3. Existe um processo de atualização de senhas privilegiadas

- a) Quantas vezes você já teve que mudar senhas de contas de “super usuário” baseado nos requisitos da política ou conformidade?
- b) Quanto tempo demora, para fazer este trabalho? Quantas pessoas são envolvidas?
- c) Que tipo de requisitos ou solicitações existe para mudar estas credenciais de forma recorrentes? A sua equipa é sempre capaz de cumprir?

4. Conceder acesso a outros - Firecalls

- a) Quem é acionado e/ou precisa de acesso de emergência - tipo “firecall”?
- b) Qual é o seu processo para fornecer esse acesso de emergência? Quantas vezes isso ocorre?
- c) Teve algum caso, que não foi possível cumprir este processo em tempo hábil?
- d) O que acontece se a pessoa determinada para realizar tal tarefa, não está disponível? Quanto tempo demora?
- e) Como é a documentação desses pedidos?
- f) Qual é a necessidade de alterar as senhas de uma vez?
- g) As para as credenciais são compartilhadas? Quanto tempo leva? Existem preocupações sobre a disseminação dessas credenciais?

Próximos Passos

As organizações que desejam mais detalhes sobre gestão de privilégios podem entrar em contato com a Netbr e a Lieberman Software para uma análise do software ERPM. Como resultado imediato você terá o levantamento de acessos privilegiados, como: hardware, conta e tipo de serviço. A análise do ERPM está disponível sem custo para as organizações qualificadas. Para mais informações, acesse nosso site: www.netbr.com.br