Arquitetura de segurança

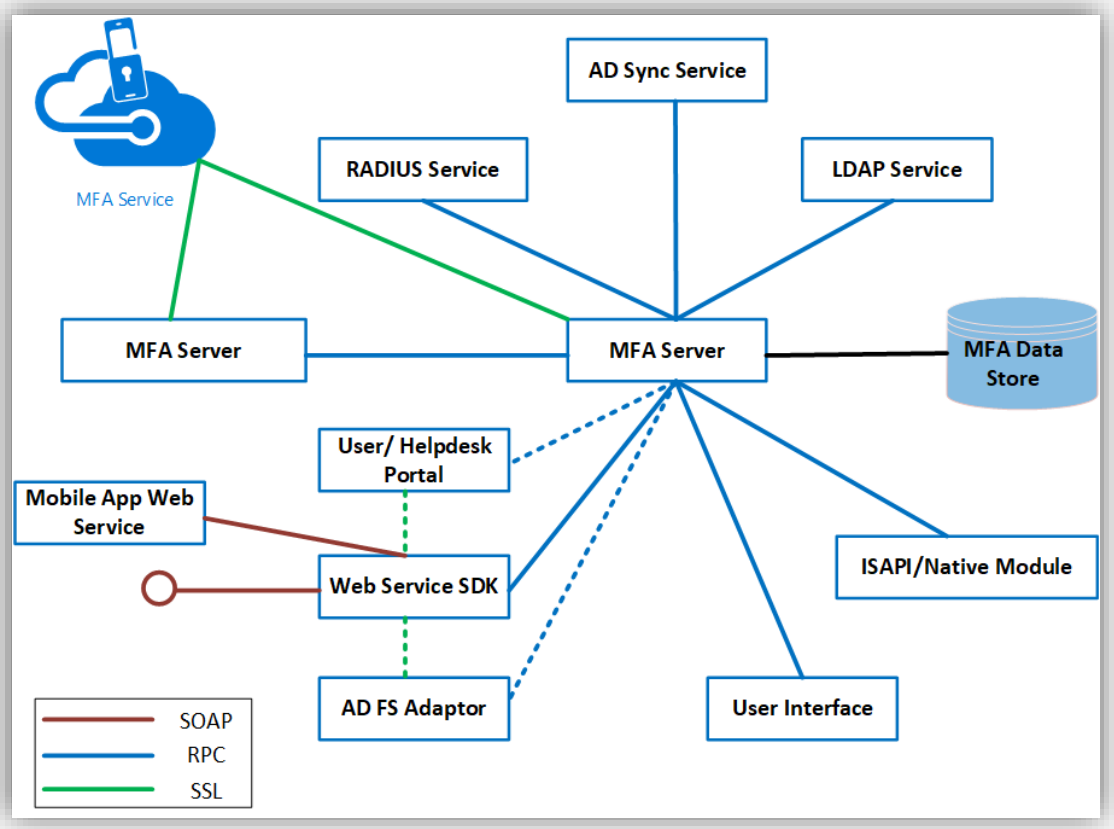
Ameaças arquiteturais – Discussão de exemplos

Ameaças de controle de acesso

Ameaças de ataques aos sistemas de controle de acesso são as mais clássicas das ameaças.

Basta existir um sistema de controle de acesso e os atacantes irão tentar "quebrar" o sistema de controle de acesso, fazendo-se passar por usuários legítimos e, executaram seus ataques usando a própria lógica de negócio das aplicações, principalmente abusando de relações de confiança da aplicação.

Exatamente por isso o problema de controle de acesso deixou de ser uma ameaça a "autenticação e autorização do sistema" e passou a ser o problema da arquitetura de controle de acesso.

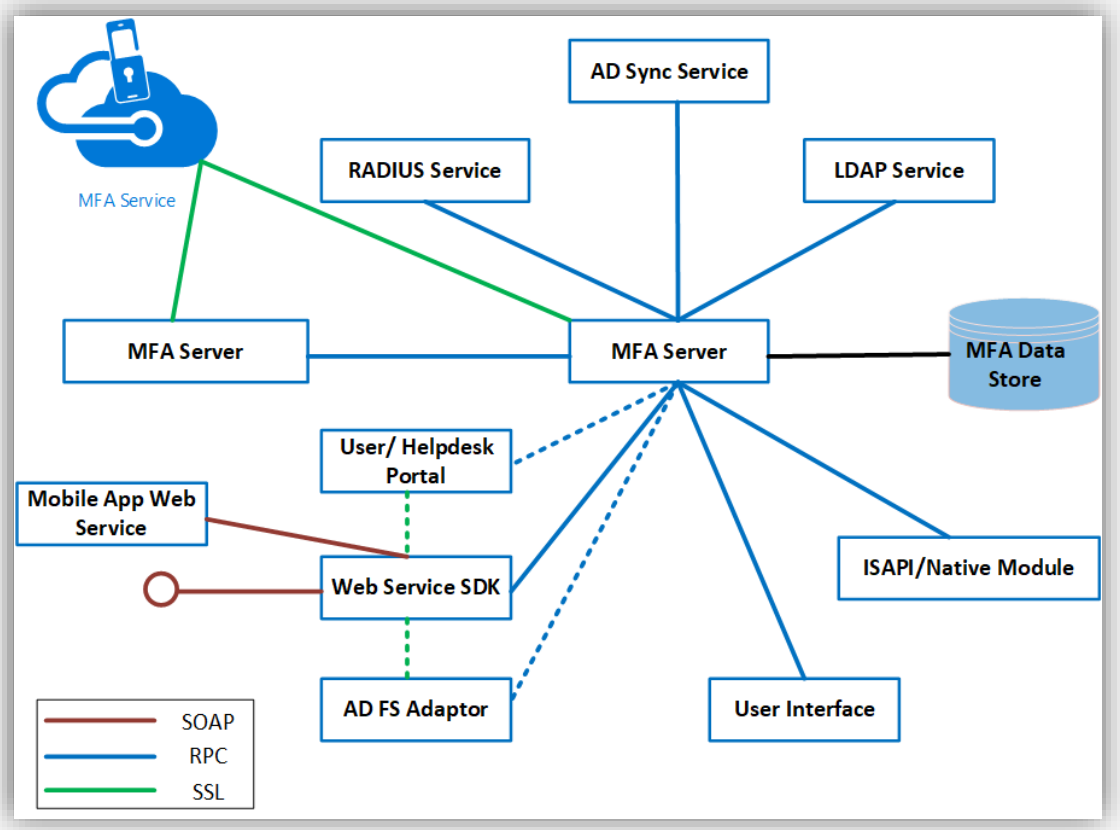


Ameaças de controle de acesso

Toda vez que tratamos de arquiteturas com múltiplos fatores de autenticação estamos exponenciando o poder de proteção do controle de acesso.

Ao lado temos um exemplo de uso de MFA que oferece um excelente nível de proteção por um lado, mas, aumenta a complexidade arquitetural de processos por outro.

Incorpora-se todos os processo que tratam do uso, desativação, troca do MFA e mesmo da recuperação de conta que muda drasticamente.



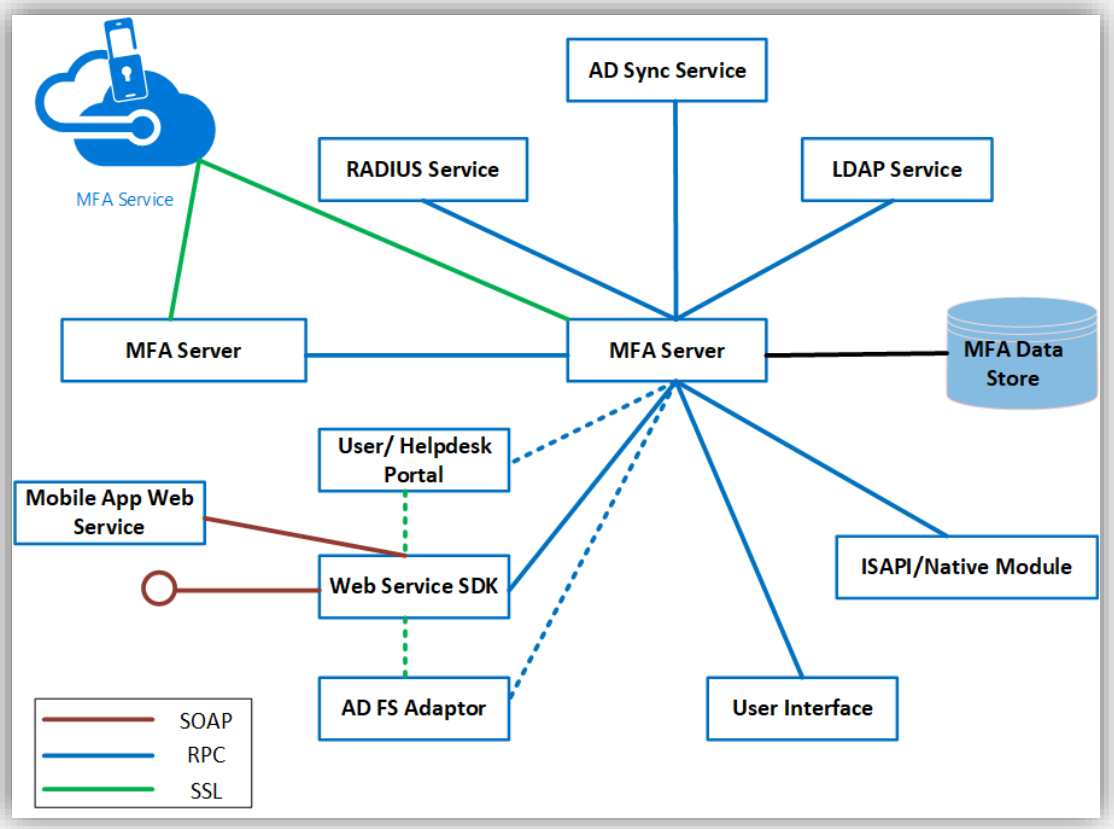
Ameaças de controle de acesso

Todos esses processos devem ser mapeados e modelados em termos das ameaças e em termos da resposta a incidentes.

Por exemplo, um sistema cujo MFA está sendo atacado e se encontra "incapaz" (DOS) de autenticar os usuários.

O Atacante conseguiria causar uma negação de serviço atacando uma integração mal desenhada destes componentes.

Ou seja, a estrutura que protege a aplicação tem suas próprias necessidades de proteção.

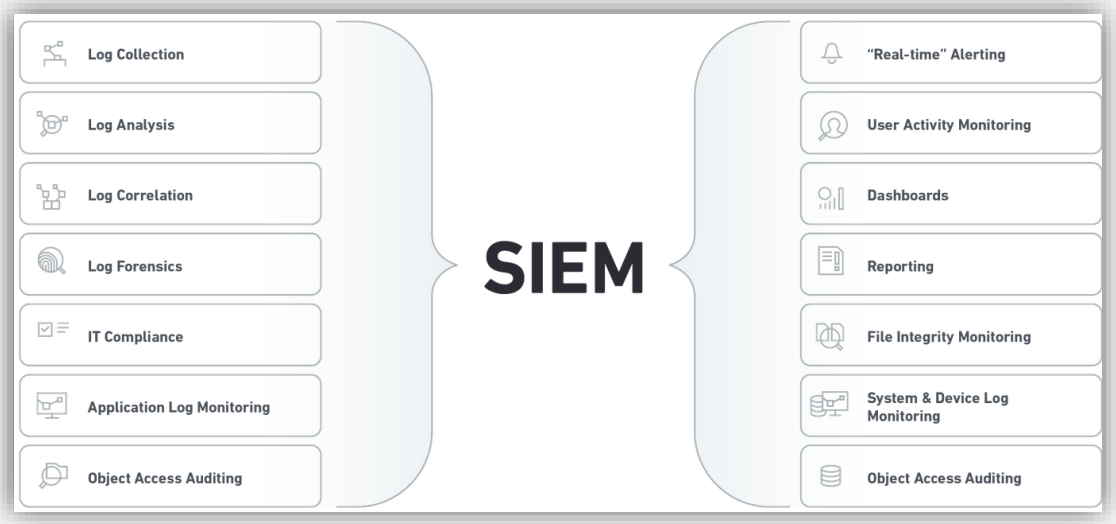


Ameaças de monitoração e logs

Os logs e o próprio sistema de correlação estão sujeitos a serem atacados assim como controle de acesso.

Caso o atacante identifique a resposta automatizada de certos incidentes/ataques e já tem certa visibilidade de cenários que disparam a resposta a incidente, ele pode disparar cenários de “cortina de fumaça”, simplesmente por saber que “manterá ocupado” o time de resposta a incidente enquanto ele efetua ataques ao alvo primário.

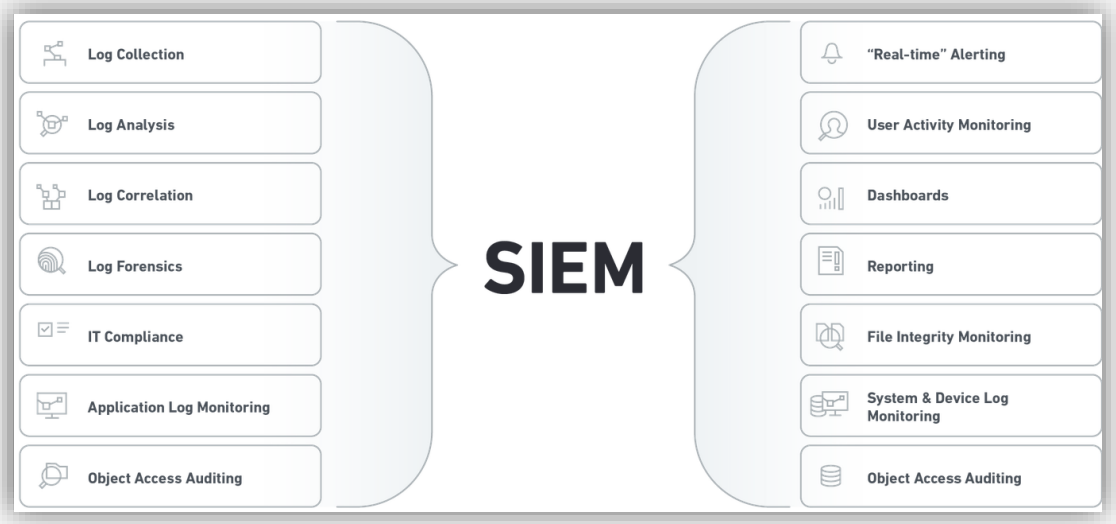
Isso seria um DOS do time de resposta a incidentes em si.



Ameaças de monitoração e logs

Mesmo que o ataque real seja registrado, por ter causado a "exaustão dos recursos humanos" da resposta a incidente, o atante tem a chance de efetivar seu ataque se agir em tempo hábil.

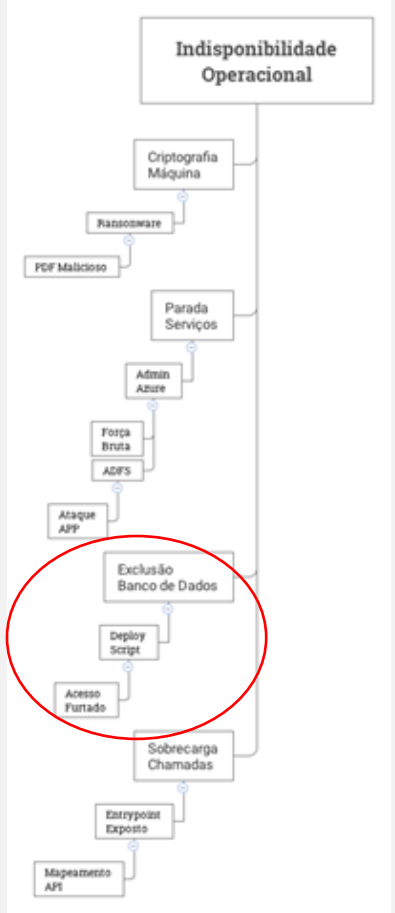
Portanto a resposta a incidente só se torna efetiva sem além do planejamento dos sistemas, houver o planejamento dos processos em três diferentes frentes: "detecção", "contenção" e "análise de causa raiz" (que retroalimenta as duas fases anteriores).



Ameaças de monitoração e logs

Por exemplo, através de um acesso ao banco de dados (seja acesso direto ao banco com a credencial, seja através do envio de comando por uma aplicação vulnerável), seguido da implantação de um script para excluir o banco de dados (permitindo que o atacante não precise mais do acesso ao ambiente e que ainda exerça seu poder de extorsão desativando o script através de pagamento).

Isso pode ser implementado com o script "policiando" um local na Internet não existente, caso esse local da Internet seja encontrado (criado pelo atacante mediante pagamento), o script se auto removeria.



Ameaças de monitoração e logs

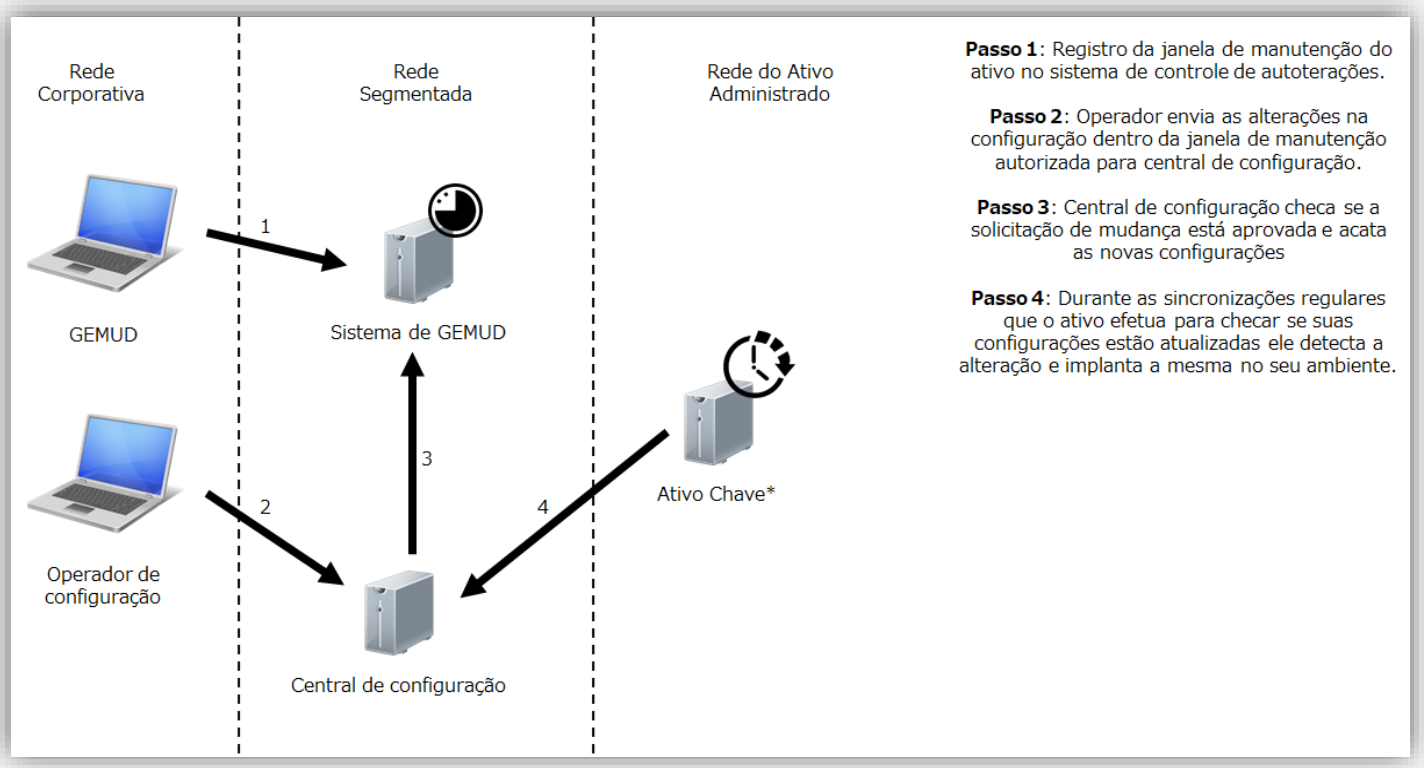
Neste exemplo, a exclusão do BD ocorre em minutos. Assim, uma medida automatizada na camada imediatamente anterior do ataque, foi adotada (momento do deploy do script para execução da chantagem).

Para conter o ataque, ao se detectar um deploy de um novo objeto, uma verificação contra uma base de scripts é disparada e se não for encontrado na base de scripts autorizados, o mesmo é removido do banco de dados – processo de verificação contra um inventário de controle.

Ameaças de monitoração e logs

Neste caso, para anular a ameaça, efetua-se a verificação de integridade, que confia em uma base de configuração que é protegida pelo sistema de GEMUD. Para ser bem sucedido no ataque, o atacante teria que quebra uma dúzia de processos e controles.

Ao introduzir esses processos e, logs gerados por eles, o arquiteto deu ao sistema de monitoração tempo e condições de identificar o atacante antes do ataque crítico.

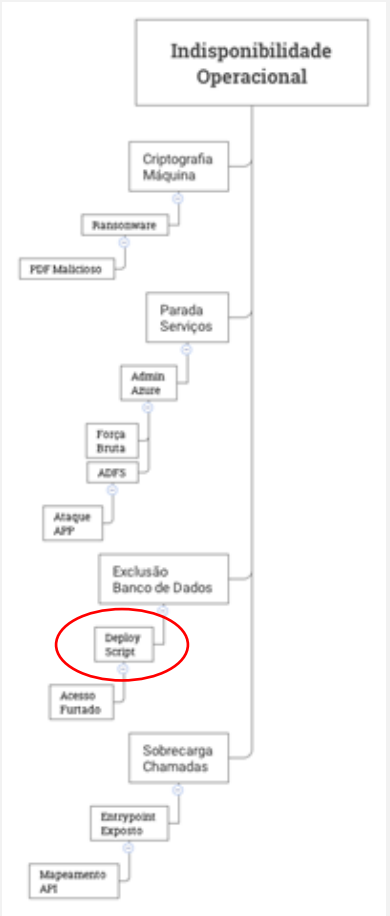


Ameaças de monitoração e logs

O atacante pode optar por atacar a relação de confiança e incluir seu script no repositório de configurações, tornando a verificação de integridade inócua (mas para isso precisaria quebrar uma série de controles)

Ou pode impedir que a consulta a base ocorra com sucesso, fazendo com que a medida de contenção/monitoração tome decisões erradas, forçando assim sua desativação temporária (ao não acessar a base de configuração, desativam-se todos os scripts causando operacionais).

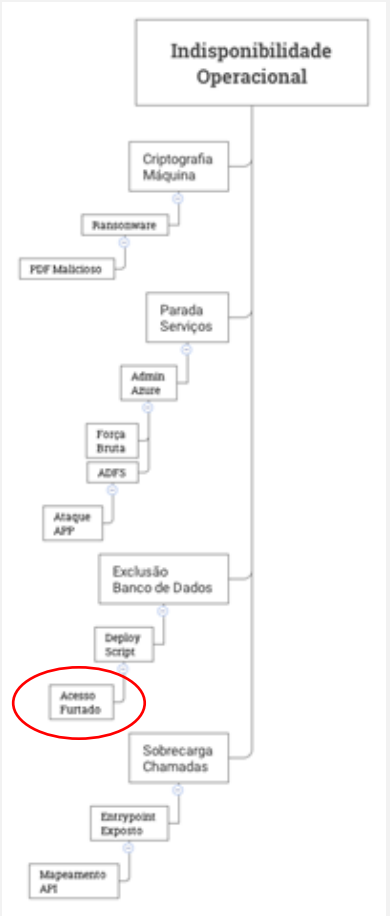
Ou seja, se as decisões automatizadas não tiverem uma implementação bastante robusta, podem ser usadas para causar distrações ao time de resposta a incidentes, gerando ruídos operacionais que impedem a resposta a incidentes eficaz.



Ameaças de monitoração e logs

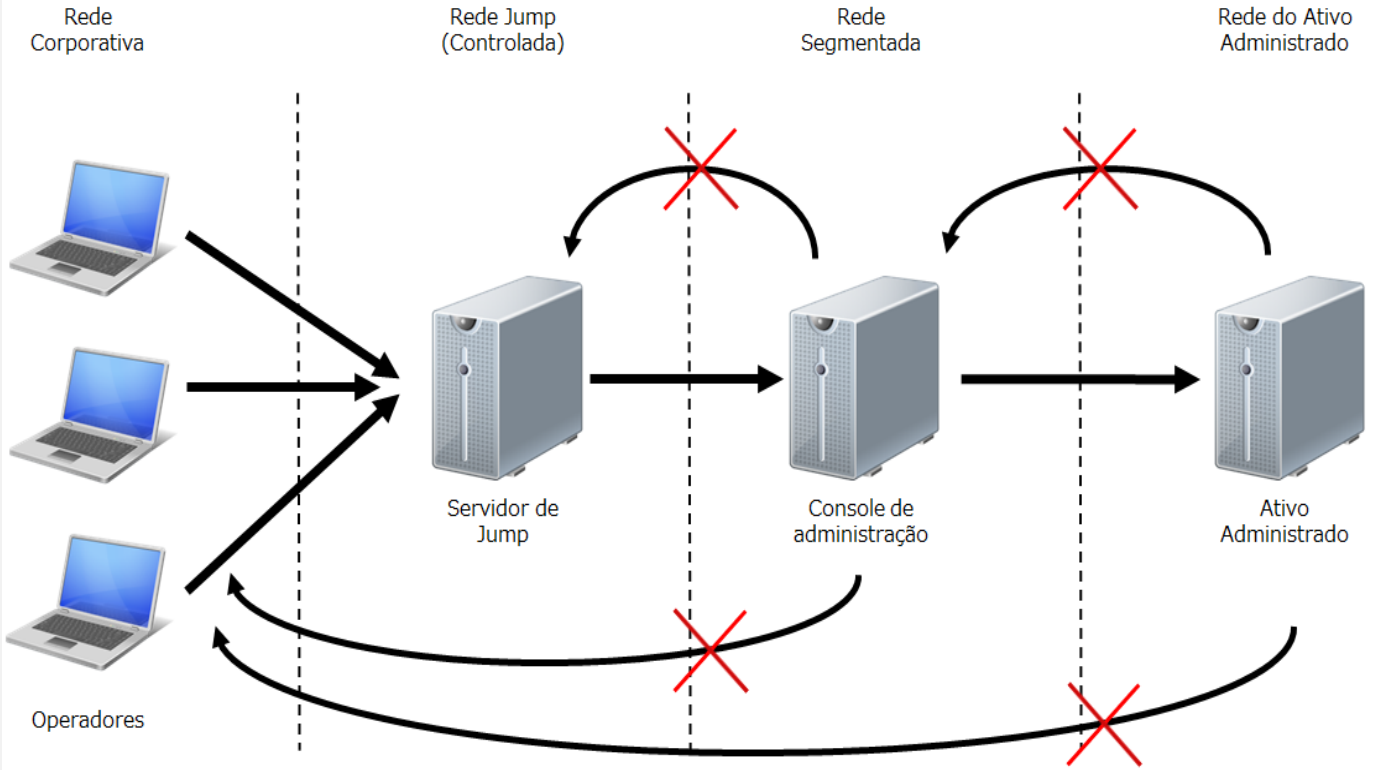
A análise do grafo de ameaças mostra a possibilidade de implementar-se ações de contenção e monitoração em ações preliminares do atacante (ele tem pouca possibilidade de causar dano real e acaba causando muito "barulho" no ambiente, facilitando sua detecção).

Isso reforça o ponto sobre o controle de acesso. Se existir um processo robusto de detecção de vazamentos e usos não autorizados de contas, com respectiva ação de bloqueio e troca de credenciais de forma automática, o vazamento não trará dano real.



Ameaças de monitoração e logs

Criar condições de detecção rápidas e eficazes, traz de novo a responsabilidade das decisões de arquitetura que tornam os acessos muito específicos e controlados, até mesmo aos serviços em nuvem. Como por exemplo, usando estações de jump-server.



Ameaças arquiteturais

Conclusão

- Controle de acesso
- Relações de confiança entre componentes
- Loging, detecção, contenção e análise em profundidade.

Esses três aspectos são os aspectos arquiteturais mais atacados de maneira geral. Portanto, cabe a equipe de arquitetura orquestrar essas necessidades entre os desenvolvimentos de aplicações, concebendo não só a arquitetura funcional, mas a arquitetura que suporte efetivamente esses três processos operacionais. Sem isso os atacantes continuarão a ter a vantagem sobre as equipes de segurança, simplesmente pela inviabilidade técnica de se detectar e rechaçar os incidentes de forma consistente.