UnB

FT – ENE
SDR

Tarefa
Questão de Estratégia Geral de Defesa

Mateus Leite Pedrosa- 17/0110842
Pedro Henrique Dornelas Almeida- 18/0108140
Diego Martins de Oliveira – 16/0049300

A estratégia do Castelo Medieval é baseada em um sistema de defesa em várias camadas, nas quais são criadas de forma independentes dificultando a invasão por ter um efeito muito negativo no invasor, pois após conseguir passar por uma camada, ele verá outra, de complexidade e resoluções diferentes, assim a cada camada é um desafio diferente. Como exemplo temos um castelo medieval de fato e ele contém 6 camadas de proteção: 1) localização(natureza);2) acessar o castelo (muros, defensores, barreiras); 3) Ponte Levadiça; 4) Muros complementares(interno/externo); 5) área interna; 6) torre principal, que é de fato aonde ficam os recursos, e para chegar até lá tem muitas camadas e dificuldades, assim também é feito em tecnologia para proteger recursos e informações importantes.

A confiança zero parte do princípio de fazer uma avaliação contínua de cada conexão que permite acesso aos recursos da empresa. Assim, a estratégia se baseia em “não acredite em nada, verifique tudo”, independente de quem seja, podem ser funcionários, parceiros, clientes, fornecedores, independente do grau que contém no acesso aos recursos. Isto também é feito para dispositivos, aplicativos, redes, fazendo com que em cada conexão a proteção seja ajustada de forma dinâmica e com base no perfil de risco. Para este modelo existe um conflito importante em arquiteturas BYOD (Bring Your Own Device), em que por exemplo cada funcionário leve seus próprios dispositivos para o ambiente de trabalho, este tipo de arquitetura não tem espaço junto ao modelo baseado em Zero Trust.

O modelo de segurança do tipo micro segmentação permite com que os arquitetos da rede dividam logicamente as aplicações, data center, base de dados, em segmentos de segurança diferentes, até chegar a um nível de divisão individual, de forma que cada máquina, cada serviço terá uma política de segurança diferente de acordo com a necessidade de acesso. Assim cada serviço ou máquina será autorizado a se comunicar somente dentro do segmento que está inserido e não pode se comunicar com uma aplicação fora do segmento. Isto permite que caso algum ataque esteja acontecendo, a rede não será afetada como um todo e sim apenas uma pequena parte da rede. Isto facilita o trabalho dos administradores para detectar invasões e controlá-las mais rapidamente sem que ela se escale para diversas áreas da rede, isto é o que chamamos de evitar uma lateralidade do ataque.

Note que estas estratégias podem se complementar caso sejam usadas em conjunto, por exemplo, utilizar um modelo de confiança zero não limita a

possibilidade de termos micro segmentação da rede, de termos várias camadas de proteção para que os recursos principais sejam acessados e podemos fazer a mesma análise para as 3 estratégias, uma não limita a implementação da outra e sim se completam.

Também é importante falar sobre a necessidade de termos estratégias de defesa, pois cada dia mais as informações são armazenadas em serviços de rede, em ambientes corporativos, e em vários cenários que contém dados e serviços mais importantes, que podem causar sérios danos caso sofram um ataque ou algo do tipo.