RELATÓRIO DE AUDITORIA

INTRODUÇÃO

Em 14 de setembro de 2022, as 16:00 horas, através de reunião virtual utilizando a plataforma Zoom, contando com a participação de Fábio Vilas Boas da *MOBTEX*, empresa contratada e responsável pela plataforma a ser utilizada, os senhores Ronaldo Bispo Lima e Miguel Messias, representantes da OAB, Marcelo Antônio Sampaio Lemos Costa, auditor responsável pela avaliação de infraestrutura e Tássio Cerqueira Dias, responsável pela avaliação do sistema, reuniram-se para apresentação da nova estrutura do sistema *Votus* e da estrutura tecnológica disponibilizada para realização do pleito do Quinto Constitucional de 2022. Após a apresentação, foi marcada uma nova reunião, desta vez presencial, onde foi apresentada e comentada a estratégia a ser adotada na data da votação, agendada para 18 de outubro de 2022. Nesta mesma reunião foi acertado os seguintes pontos: A *MOBTEX* disponibilizará o ambiente da AWS para efetuar testes de penetração, enviando 5 *e-mails* para teste real da aplicação e descrição da estrutura e configuração da *AWS* para o auditor Marcelo. Fica também acordada uma reunião posterior para testes de stress com a base de dados final de produção e uma nova visita à sede da *MOBTEX*, no dia 19/09 às 14 horas, para análise do código fonte do sistema. Foram definidos prazos para a realização de tais ações.

OBJETIVO

Este trabalho objetiva avaliar a infraestrutura escolhida e suas configurações, para verificar sua adequação à proposta do serviço e sua capacidade de responder a possíveis incidentes.

INFRAESTRUTURA PROPOSTA

Conforme informado pela *MOBTEX*, através de uma apresentação e de uma lista enviada por e-mail, serão utilizados os serviços da *Amazon Web Services,* que oferece uma infraestrutura bastante robusta para o serviço proposto. A proposta, conforme

apresentada na reunião, é diferente da utilizada no pleito anterior, ainda que baseada na *AWS*, acrescentando alguns itens voltados para garantir ainda mais a segurança e disponibilidade.

De acordo com os diagramas apresentados observou-se que, como no último pleito, a proposta utiliza o *Amazon EC2*[1] *(Elastic Compute Cloud)* incluindo serviços de *ELB*[2] *(Elastic Load Balancing), Amazon Route 53*[3] e *AWS Shield*[4].

O *EC2 (Elastic Compute Cloud)* é um serviço que oferece escalabilidade de recursos baseado em demanda, fornecendo instâncias de acordo com o fator de solicitação configurado. Uma instância consiste em uma combinação de CPU, memória, armazenamento e rede, em capacidades variadas a escolha e que pode conter mais de um tamanho de instâncias. Conforme as informações prestadas pela *MOBTEX* serão utilizados, inicialmente, dez containers *EC2* que serão escalados automaticamente caso atinjam 50% de sua capacidade.

O *EC2 Auto Scaling* permite a escalar de forma automática a capacidade baseada na configuração definida, mantendo a disponibilidade da aplicação. Conforme as informações prestadas pela *MOBTEX* o contrato não possui limites, escalando sempre que necessário.

O *ELB (Elastic Load Balancing),* atua de acordo com o nível de requisição, distribuindo automaticamente o tráfego de entrada para o conjunto contratado, distribuindo a demanda da aplicação, rede, etc.

O *AWS Shield* é um serviço gerenciado de proteção contra ataques de Negação de Serviço Distribuído, conhecidos como *DDoS (Distributed Denial of Service)*, produzidos para submeter rapidamente um servidor ao seu limite de capacidade de atendimento.

---

[1] *EC2* – Estrutura escalável e redimensionável sob demanda que permite sua expansão de forma simples e rápida de acordo com quanto for requisitado pelo serviço.
[2] *ELB* – Serviço de balanceamento de carga seja de tráfego *HTTP/HTTPS (Application Load Balancer)*, tráfego de *TCP/TLS (Network Load Balancer)* ou balanceamento básico entre instancias do *EC2.*
[3] *Amazon Route 53* – Serviço de *DNS (Domain Name Service)*.
[4] *AWS Shield* – Serviço de proteção adicional a ataques DDoS mais comuns nas camadas de rede e transporte.

O *Amazon Route 53* é um serviço de *DNS (Domain Name System)* em nuvem e alta escalabilidade, visando fornecer um serviço seguro.

Segundo a *MOBTEX*, será utilizado o *DynamoDB,* um serviço de banco de dados *NoSQL* de alta performance em qualquer escala, segundo o desenvolvedor da aplicação. Também será utilizado o *RDS (Amazon Relational Database Service)*, que é um serviço de banco de dados em nuvem, relacional e distribuído, projetado para simplificar a configuração, operação e escalonamento de um banco de dados relacional para uso em aplicativos.

Por fim será utilizado também o *WAF (Web Application Firewall) Cloudflare* apontado para o *Load Balancer da AWS*. Esta camada extra não foi utilizada no evento de 2018/2019). Isso implementa uma camada extra de segurança antes de chegar à *AWS.* A estrutura de servidores será alocada em São Paulo, reduzindo em ¼ o tempo de acesso, que cai de 200 *(USA)* para 50 milissegundos *(BRA)*.

AVALIAÇÃO

A infraestrutura oferecida é suficientemente robusta para a tarefa proposta superando as necessidades impostas.

Vale ressaltar que nenhuma infraestrutura ou aplicação está livre de ataques, entretanto, se estiver adequada, mitiga com facilidade as ações externas que possam ter interesse em prejudicar a execução do serviço de votação. Um ponto que chegou a ser abordado na reunião do dia 16/09, que é de vital importância que seja exposto neste relatório, trata da condição de segurança do dispositivo utilizado pelo usuário para fazer acesso ao sítio onde será realizado o pleito. Os acessos poderão ocorrer por diversos tipos de dispositivos como celulares, *notebooks*, etc., com a utilização de sistemas operacionais como *Android*, *Apple iOS*, *Windows*, *Apple MacOS*, *Linux*, etc., e dos diversos *browsers*, tais como o *Mozilla Firefox*, *Microsoft Edge*, *Google Chrome*, *Opera*, etc., entretanto qualquer um deles está sujeito à ação de *malwares*, especialmente aqueles que agem com redirecionadores, que podem encaminhar o usuário para destinos diversos, dificultando ou até impedindo a realização do voto, sem que isso tenha qualquer relação com a solução proposta.

Uma correta configuração do ambiente permitirá um funcionamento estável dentro do que se espera para o quanto proposto.

Finalizando, na reunião abordou-se a possibilidade de realização de um teste de negação de serviço distribuído e/ou um teste de stress, entretanto chamei a atenção de que um teste de tal natureza sobre a infraestrutura da *AWS* só pode ser realizada através de parceiros credenciados da *Amazon* e com prévia autorização. Esta questão já havia sido pleiteada na última votação do Quinto Constitucional de 2018, onde citei:

> "A infraestrutura da *Amazon Web Service* presente no Brasil, deixa de forma clara em sua política que: *"Tests that purposefully attempt to overwhelm the target and/or infrastructure with packet or connection flooding or other large volumes of traffic are not considered network stress tests but are considered distributed denial of service (DDoS) tests. Volumetric network-based DDoS simulations are explicitly prohibited from the Amazon EC2 platform.".* Em tradução livre diz que "Testes que propositalmente tentam sobrecarregar o alvo e/ou a infraestrutura com inundação de pacotes ou conexões ou outros grandes volumes de tráfego não são considerados testes de estresse da rede, mas são considerados testes de negação de serviço distribuído *(DDoS)*. As simulações *DDoS* volumétricas baseadas em rede são explicitamente proibidas na plataforma *Amazon EC2.""*

Sem a autorização devida, que exigiria tempo e recursos outros, incorreríamos no crime de "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública."

> "O §1º foi incluído pela Lei nº 12.737/2012 ficando:
>
> *"Art. 266 – Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:*
>
> *Pena – detenção, de um a três anos, e multa.*
>
> *§1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.*

§2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.""

Por fim foram realizadas prospecções no site disponibilizado para o pleito, sito na *URL https://oab-validation.votus.app*, através de scanner de vulnerabilidades em busca de fragilidades exploráveis, entretanto as configurações aplicadas à plataforma para os ataques mais utilizados na atualidade, seja para negação de serviço distribuído, como para *sql injection*, manipulação de *URL*, etc., não apresentavam vulnerabilidades conhecidas.

SUGESTÕES

Sugiro algumas medidas que considero relevantes diante da importância do evento, de forma a subsidiar qualquer apuração/investigação relacionados aos resultados do pleito e para o caso de incidentes durante sua execução.

1. Preservação através de cópia das máquinas virtuais utilizadas durante o pleito;
2. Preservação dos *logs* de todos os recursos utilizados na infraestrutura, desde o *Cloudfllare* até a estrutura final *AWS;*
3. Os dados coletados deverão ser gravados em mídia e apresentados em conjunto com um relatório, consignando com os valores de *hash SHA-256* para cada arquivo preservado.
4. O material deverá ser descartado de acordo com definições a serem estabelecidas pela OAB.

CONCLUSÃO

Concluindo o presente relatório, podemos atestar que a infraestrutura proposta pela *MOBTEX* oferece condições de mitigar possíveis ataques.

Salvador, 20 de setembro de 2022

Assinado de forma digital por MARCELO ANTONIO SAMPAIO LEMOS COSTA:24852058504
Dados: 2022.10.12 09:33:47 -03'00'

Marcelo Antonio Sampaio Lemos Costa