PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Av. Brasil, 2023

Funcionários, Belo Horizonte – MG – CEP 30040-002

IMPLEMENTAÇÃO DE UMA REDE SEGURA DE COMPUTADORES

Belo Horizonte

2023

Antônio Gabriel Batista Vieira
Diogo Junio Pinheiro dos Santos
Everton Rezende Spadaccini
Gustavo Felipe Borges Pereira
Luiz Gustavo Giovanini

IMPLEMENTAÇÃO DE UMA REDE SEGURA DE COMPUTADORES

Projeto apresentado ao curso de graduação de Redes de Computadores da Instituição Pontifícia Universidade Católica de Minas Gerais, com objetivo de implementar medidas de segurança em uma infraestrutura de redes.
Orientador: Luiz Alberto Ferreira Gomes.

Belo Horizonte

2023

Sumário

Introdução

O objetivo desta etapa é a criação de um projeto de rede segura onde será implementado um workflow de etapas para a garantir a disponibilidades e segurança dos serviços apresentados pela equipe de TI.

Serão utilizadas implementações de segurança em todas as camadas de segurança começando na infraestrutura em cloud até o usuário final, este processo visa resguardar os dados da empresa e a lisura dos processos, ficando em conformidades com as leis da LGPD.

1. Avaliação da Infraestrutura existente

O modelo atual de infraestrutura é composto por servidores locais (on-primese) e algumas máquinas virtualizadas (VMWARE), sendo todos eles gerenciados pela própria organização. Neste modelo, todas as implementações, manutenções e gerenciamento de hardware e softwares são feitos pela equipe de TI da empresa. Após uma análise completa foi verificado inúmeros problemas, como por exemplo: Falta de escalabilidade para serviços, licenças vencidas, cronograma de manutenções defasado assim como o de atualizações, além de upgrades de hardware necessários para continuidade nos negócios.

Desta maneira este projeto visa a implementação uma solução de monitoramento, de toda a infraestrutura que atualmente está alocada de modo virtual, em nuvem publica na AWS (Amazon) com modelo de serviço IaaS, escalonamento sob demanda, construção de um cronograma para manutenções, atualizações e upgrade, infraestrutura de backup seguro, criptografia, segurança de rede além de programas de instruções e treinamentos para os usuários.

2. Implementação de Firewalls

Problema:

Após análise minuciosa das configurações dos firewalls internos e de borda foram encontradas algumas vulnerabilidades, dentre elas estas a seguir:

- Bloqueio de “rotas” configuradas incorretamente, o que pode gerar tráfego indevido de origens desconhecidas. Esta ameaça acontece quando um terceiro intercepta um tráfego de rede redirecionado por um link de indexação de pesquisa dos sites de busca, evitando assim o usuário acessar sites com propagandas indesejáveis.

Solução:

Após análises e testes foi realizado um levantamento de sites potencialmente perigosos com conteúdo indevido. Foram listadas categorias para mapeamento e bloqueio destes sites:

- Livestreeam e jogos;
- Sites de Apostas;
- Conteúdo Adulto;
- Extensões disponíveis do navegador;
- Download de Torrents;
- Sites sem certificação SSL.

Para o bloqueio de sites utilizamos o serviço nativo da AWS o AWS WAF, que é um firewall de aplicativo web que permite monitoras as solicitações HTTP e HTTPS encaminhadas paras os recursos de nossa infraestrutura. Dentre as opções de bloquei utilizamos duas regras que melhor se encaixam no cenário acima:

- Permitir todas as solicitações, exceto aquelas especificadas;
- Bloquear todas as solicitações, exceto aquelas que você especificar.

Para monitoramento de tráfego da rede e comportamento de filtragem utilizamos o AWS FIREWALL NETWORK. Com isso, tanto as regras do cliente quanto os logs de acesso são criptografados em repouso e em trânsito entre os serviços da AWS subjacentes, além da implementação das ACLs para controle de acessos a níveis de subrede.

3. Controle de Acesso a Rede

Problema:

A infraestrutura atual não conta com autenticação de múltiplos fatores, além disso não há um padrão de complexidade para as senhas dos usuários. Outro fator importante é a criação de grupos para a restrição de responsabilidade entre equipes e para finalizar a criação de uma network ACL, controle de acesso a rede baseado em regras.

Solução:

Habilitar a política de autenticação por múltiplo fator, definir um padrão de complexidade elevado para as senhas dos usuários, criar grupos e equipes para definição de permissão e responsabilidades. Para realização dessas funções, utilizamos o serviço nativo da AWS o AWS Identity and Access Management (AWS IAM), que especifica que ou o que pode acessar os serviços e recursos na AWS, gerenciar permissões refinadas de maneira centralizada além de analisar o acesso habilitar a múltipla autenticação para as contas.

4. Criptografia

Problema: A criptografia deve ser habilitada tanto na tratativa dos dados quando no seu transporte, desta maneira necessitamos que haja uma comunicação segura em conjunto com o armazenamento dos dados.

Solução: A solução descrita aqui pode ser com a tratativa de implementar o TLS (Transport Layer Security) para criptografar os dados em transporte, fazendo assim, que fique seguro a transmissao dos dados em tempo real. Outra sugestão, seria a criação de um servidor apache para gerar certificados de segurança, fazendo com que nossa conectividade utilize o protocolo HTTPS para comunicação WEB.

5. Monitoramento e detecção de intrusões

Problema:

A infraestrutura contava com um software de monitoramento free, onde o número de sensores é limitado, desta maneira resolvemos investir em um monitoramento nativo da plataforma, além de habilitar alarmes para possíveis invasões ou falhas de segurança através do Zabbix para realização do monitoramento ostensivo, apartado da AWS.

Solução:

Ao utilizarmos o Zabbix como monitoramento, podemos utilizar ele em sua estância EC2, já que no marketplace, teríamos mais um custo adicional na rede. Com o Zabbix totalmente implantado, podemos configurá-lo para fazer o monitoramento total da nossa rede, seja interna como tentativa de invasão externa via firewall.

Para monitoramento da infraestrutura cloud, contamos com o serviço nativo da AWS, o AWS CLOUDWATCH, ele monitora os recursos e aplicativos da AWS em tempo real, além de rastrear e coletar métricas.

6. Treinamentos e divulgação

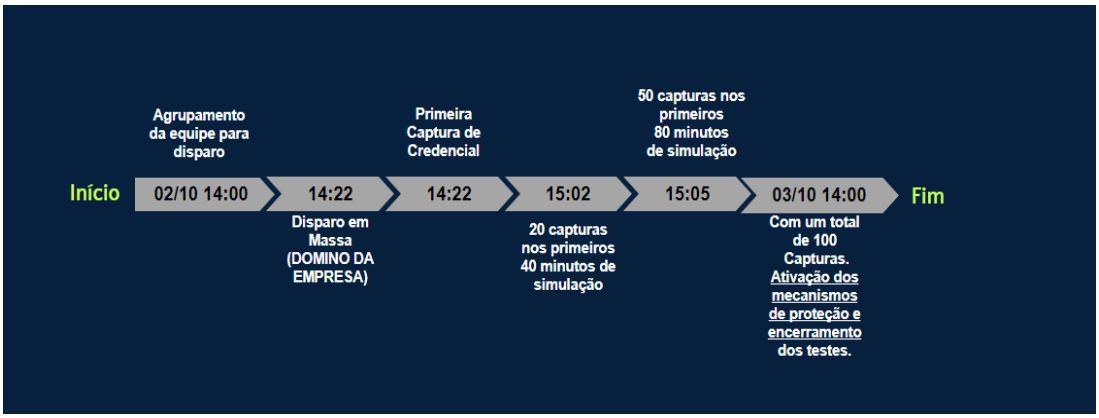
Problema: A conscientização e treinamento foi restruturada já que a política anterior se encontra defasada com relação a recursos e boas práticas. Desta maneira reforçamos o envio de e-mails de conscientização reuniões trimestrais além de uma caixa de dúvidas e sugestões abertas aos funcionários, trazendo maior proximidade e conhecimento para todos.

Solução: Realizar treinamento com usuários periodicamente, por exemplo, a cada 3 meses. Fazer envio de e-mail e palestra de conscientização. Deixar em aberto uma caixa de dúvida, sugestão, melhoria para podermos avaliar melhor e entender melhor onde o usuário se sente mais protegido e mais defasado. E por final, deixar tudo documentado e compartilhado com os usuários de segurança da informação.

O Phishing trata-se de um método de captura de credenciais, vitimando usuários vulneráveis, a fim de obter acesso a contas de e-mails, sistemas, redes corporativas. A partir desse ataque terá informações para diversos ataques como, invasões sequestros de informações, criptografia de dados e até mesmo ações destrutivas do parque tecnológico atacado.

Sendo assim foi realizado um teste de intrusão pelo time de segurança, para conscientizar todos os colaboradores da empresa, justamente utilizando o método de captura de Phishing para testar o nível de maturidade de nossos usuários e sistemas de segurança cibernética,

Encaminhamos um e-mail “OFERTAS PROMOCIONAL” a todos os colaboradores que possuem contas válidas da empresa, com o intuído dó usuário realizar o cadastro da oferta, é encaminhado para um site falso a qual solicita a autenticação de usuário e senha, com isso temos todos as permissões do usuário.



Resultado.

1. Em aproximadamente 24 horas de teste foram coletadas 100 credenciais ativas.
2. 150 ocorrência de abertura do link do site (click)
3. Dos 100 usuários que informarão as credenciais, 0 realizaram a alteração de senha.

Sendo assim foi orientado a todos os colaboradores que acabaram compartilhando suas credenciais a realizar um treinamento breve sobre cyber segurança, onde exibimos alguns métodos de prevenção aos ataques dos invasores.

Encaminhamos vídeos semanalmente na caixa de e-mail corporativo da empresa para conscientização de todos os colaboradores tomarem cuidado com alguns tipos de ataques que são mais acostumados a conter em um ambiente corporativo, segue abaixo alguns vídeos de exemplos.

Após o término dos treinamentos dos vídeos para os colabores que acabaram compartilhando suas credenciais, foi enviado um formulário com algumas perguntas sobre alguns ataques mais utilizado pelos hackers.

7. Testes de Penetração (Pentest)

7.1. Teste de aplicativos WEB (BlackBox)

Este teste de penetração foca em avaliar sites e aplicativos fornecidos através da web e internamente na infraestrutura da empresa, visando diminuir os riscos de um possível ataque proveniente da internet ou um ataque interno, no cenário atual os servidores web estão localizados em uma sub rede (DMZ) pública, facilitando a sondagem para eventuais falhas de desenvolvimento, codificação e infraestrutura que possa apresentar algum risco a segurança.

O teste é realizado através de informações como: Range de IP, tabelas de usuários, páginas estáticas e dinâmicas e campos de entradas.

O Pentest tem como foco buscar vulnerabilidades nas camadas entre a infraestrutura lógica e os serviços implementadas dentro da infraestrutura.

- Ping da Morte: Objetivo deste teste será deixar indisponível os links da rede, deixando os serviços inativos;
- Port scann: Este teste terá o objetivo de realizar a sondagem das portas TCP em modo "listening" e testar conexões UDP em portas passiveis de vulnerabilidades após análise dos fluxos de tráfego da rede, sondagem do possível servidor que hospedará os serviços e aplicações diretas e indiretamente ligadas aos serviços utilizados.
    - Serviços diretos: Servidor WEB, Banco de Dados, código fonte dos sites hospedados, entre outros;
    - Serviços Indiretos: Client DNS, serviços SMB para compartilhamento interno de arquivos, serviços FTP, Telnet entre outros que possam gerar vulnerabilidade.

7.2. Engenharia Social (Greybox)

Com este teste é avaliada a capacidades dos funcionários em analisar, identificar e reportar eventuais ataques de phishing via e-mail.

O teste deve ser realizado após uma campanha efetiva de prevenção e phishing, com boas orientações e conteúdo abrangente. No próximo tópico entraremos em maiores detalhes sobre o treinamento e prevenção a phishing.

Os modelos de utilizados para o teste de penetração foram o **Blackbox**, o teste que é realizado quase sem informações, de modo externo e que na maioria dos casos gasta maior tempo para execução. E o Greybox, que consiste em uma mistura de Whitebox e Blackbox, o ataque é realizado de forma interna e externa, neste caso é realizado um estudo prévio onde as informações são levantadas e analisadas.

7.3. Fases de teste de penetração

7.3.1. Reconhecimento do Alvo, avaliação de riscos e vulnerabilidades.

A fase do reconhecimento é a primeira fase, onde o atacante levanta e analisa o maior número de informações possíveis, para que o ataque seja bem-sucedido, o atacante busca verificar quais componentes são importantes e como eles devem ser explorados.

7.3.2. Fase de Exploração

Investigação completa da rede, utilizando técnicas de scan e outras ferramentas para levantamento de informações.

7.3.3. Coleta de evidências

Indicação de todas as falhas e problemas identificados durante as etapas anteriores, destacando a existência das mesmas e possíveis riscos futuros.

7.3.4. Relatórios

Documentação detalhada dos processos e ferramentas utilizadas, com laudo conclusivo sobre as atuais falhas de segurança.

8. Serviços da AWS

8.1. AWS SHIELD

Para proteção contra os ataques DDoS mais comuns e acesso a ferramentas e melhores práticas para construir uma arquitetura resiliente a DDoS.

8.2. AWS CLOUD FRONT

O Amazon CloudFront é um serviço da web que acelera a distribuição do conteúdo estático e dinâmico da web, como arquivos .html, .css, .js e arquivos de imagem, para os usuários. O CloudFront distribui o conteúdo por meio de uma rede global de datacenters denominados pontos de presença.

8.3. AWS S3

O Amazon Simple Storage Service (Amazon S3) é um serviço de armazenamento de objetos que oferece escalabilidade líder do setor, disponibilidade de dados, segurança e performance.

8.4. AWS CLOUD TRAIL

Eventos do CloudTrail é o registro de uma atividade naAWSconta. Essa atividade pode ser uma ação de uma identidade do IAM ou de um serviço que seja monitorado por CloudTrail.

8.5. KMS

O AWS KMS ajuda você a criar e controlar as chaves de criptografia usadas por aplicações e serviços com suporte da AWS em diversas regiões do mundo usando um único console.

8.6. AWS CLOUDWATCH

O Amazon CloudWatch coleta e visualiza logs, métricas e dados de eventos em tempo real em painéis automatizados para otimizar sua infraestrutura e manutenção de aplicações.

8.7. AWS ELASCT LOAD BALACING

O Amazon Elastic Load Balancing é um serviço AWS de balanceamento de carga para aplicações. Ele distribui, de maneira equilibrada, cargas de trabalho, requisições e acessos a sistemas entre instâncias do EC2 (servidores AWS em nuvem), contêineres e endereços IP.

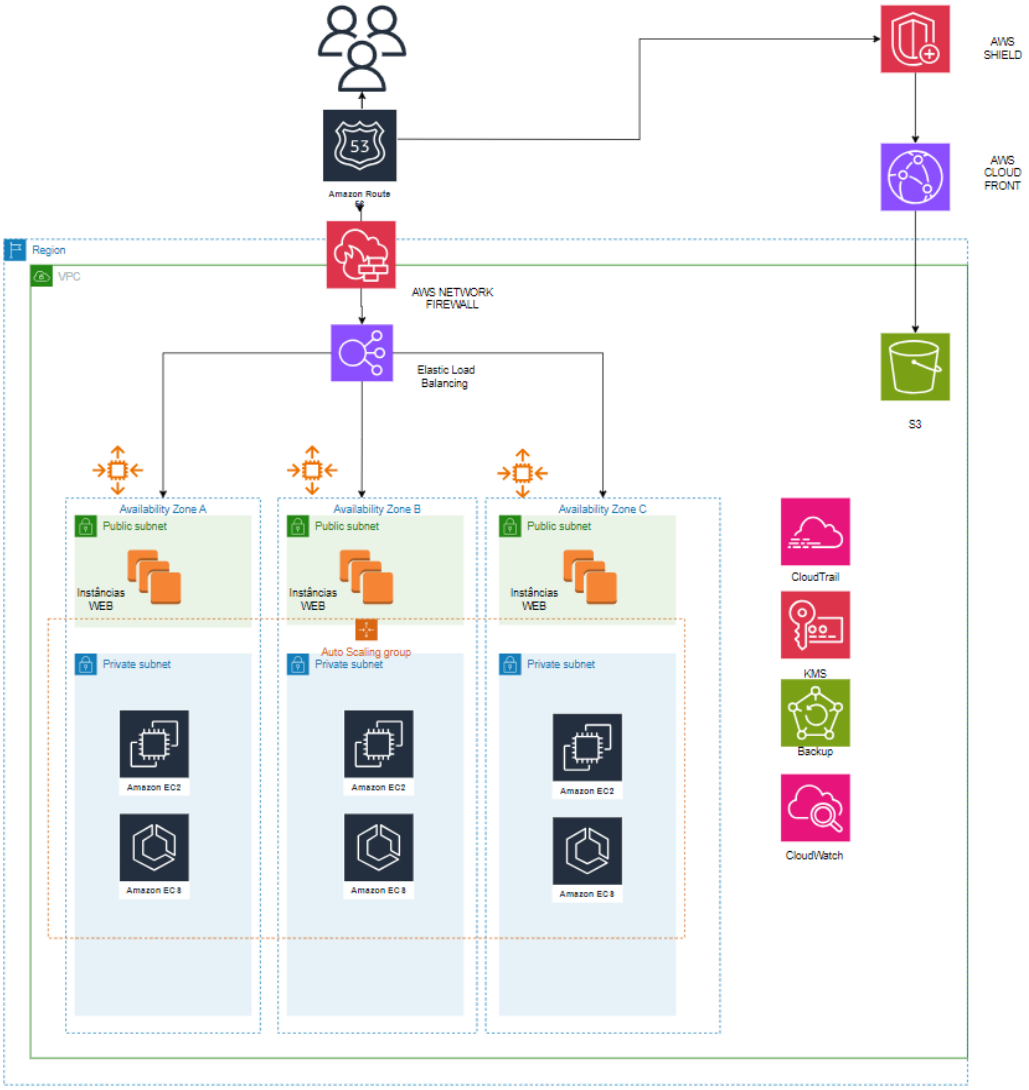
9. Fluxograma de Infraestrutura AWS

Conforme apresentado na infraestrutura abaixo, os usuários que desejam ingressar na infraestrutura AWS precisam primeiramente passar pelo Route 53, que é um serviço web de DNA altamente disponível e escalável e como funcionalidade conecta as requisições do usuário a aplicações da Internet executadas na AWS.

Desta maneira a solicitação é encaminhada para o AWS Network Firewall, que conecta uma política de firewall, definindo o monitoramento do tráfego de rede, filtragem dos dados que será encaminhado para as zonas de disponibilidades e sub-redes.

Após a filtragem realizada pelo AWS Network Firewall o tráfego de entrada é distribuído automaticamente atravé do Elastic Load Balancing entre vários destinos como instâncias do EC2, contêiners e endereços IP, em uma ou mais zonas de disponibilidade. Escalando automaticamente a capacidade do balanceador de carga em resposta a mudanças no tráfego de entrada.

A infraestrutura subjacente é formada por uma subnet publica onde estão as instâncias web e a subnet privada onde estão as instâncias EC2 e ECS (Onde estão alocados nossos servidores virtuais e banco de dados).


AWS SHIELD
AWS CLOUD FRONT
Amazon Route 53
Region
VPC
AWS NETWORK FIREWALL
Elastic Load Balancing
S3
Availability Zone A
Availability Zone B
Availability Zone C
Public subnet
Instâncias WEB
Auto Scaling group
Private subnet
Amazon EC2
Amazon EC 8
CloudTrail
KMS
Backup
CloudWatch