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 Júnio 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 criar um plano detalhado de todas as ações realizadas na implementação de técnicas para garantir a segurança da infraestrutura da rede.

Foram também relacionadas nesta etapa todas as análises realizadas para diminuir o percentual de riscos presentes na análise feita no início do projeto.

1. Revisão das medidas de segurança implementadas

Após a implementação do AWS WAF, que é um firewall de aplicativo web conseguimos proteger nossos sites de ataques comuns, como por exemplo o “SQL Injection” e o “cross-site scripting(XSS)”. Como metodologia preventiva, foram criadas regras para bloquear ataques de agentes-usuários, bots maliciosos ou contente scrapers.

Continuando na sessão de firewalls, fizemos uso do AWS FIREWALL NETWORK, visando o monitoramento de tráfego de rede e filtragem de pacotes. Tudo isso aliado a criptografia (KMS), de logs e comunicação entre serviços AWS subjacentes.

Em controle de acesso utilizamos o AWS IAM, que gerencia todas as os controles de acesso, ou seja, quem é autenticado (fez login) e autorizado (tem permissão) a usar os recursos da infraestrutura.

Para monitoramento da infraestrutura subjacente utilizamos o ZABBIX, instalado em uma instância EC2, tendo assim as informações enviadas monitoradas através de clientes em dispositivos finais, para o monitoramento da infraestrutura cloud, utilizamos o AWS CLOUDWATCH, recurso nativo da AWS que monitora as aplicações executadas em tempo real, utilizamos os painéis personalizados para exibir métricas sobre os aplicativos que achamos mais sensíveis, apresentando graficamente esses dados no console

2. Identificação de pontos fortes

Imagem 1 – Grupos de serviços AWS.

Revendo todos os pontos da infraestrutura, podemos afirmar vários pontos fortes identificados para melhor segurança e confiabilidade.

Utilizando a plataforma AWS temos como ponto e resiliência energética, escalabilidade, monitoramento nativo, CloudWatch além de controlei de gerenciamento de usuários que é o IAM, ferramentas nativas da AWS que garante uma confiabilidade muito maior.

Temos também a dupla autenticação além de ter de usar o (MFA)Autenticação multifatorial, Os Firewalls nativos de borda e interno, os ACLs, listas de controle.

Por estar na AWS, temos redundância de hardware, elétrica, internet, além de softwares de monitoramento e antivírus padronizado nos terminais e sistemas operacionais atualizados.

Escolhemos por questão de segurança somente 2 pessoas ter acesso à senha de administrador. Várias rotinas de backups e backups das máquinas virtuais. Mas além de todos os pontos fortes, temos 5 profissionais com conhecimento técnico avançado, analistas de redes e infraestrutura sênior.

Estamos em conjunto com todas as medidas técnicas, focados em palestras rápidas dentro da empresa com todos os funcionários e usuários dedicando em passar conhecimento e instruções de segurança para tornar uma cultura de conhecimento mínimo sobre segurança de rede.

3. Identificação de Vulnerabilidades e Pontos Fracos

Imagem 2 – Versão de Atualização Windows.

Após uma análise de toda a infraestrutura conseguimos identificar uma vulnerabilidade infraestrutura subjacente, especificamente nos sistemas operacionais instalados nos endpoints.

Atualmente 99% do parque máquinas possuem o sistema Windows, em versões: 1607, 1809, 21H2 e a mais atual 22H2. Para a padronização e implementação das políticas de segurança, todas as máquinas foram atualizadas para a versão 22H2 Enterprise que tem a data final de manutenção: 14/10/2025.

4. Análise de Riscos

Com base nas vulnerabilidades e pontos fracos identificados, os alunos devem realizar uma análise de riscos. Isso envolve avaliar o impacto potencial de cada vulnerabilidade e a probabilidade de ocorrência de um incidente de segurança. A análise de riscos ajudará a priorizar as ações corretivas e a determinar quais medidas de segurança devem ser implementadas ou aprimoradas.

Após feito essa análise minuciosa citada acima, identificamos que seria a atualização do parque todo através de GPO no servidor, datado para um final de semana em que não impacte a operação da empresa. Será 2 (dois) dias de atualização e disponibilização das máquinas para operação novamente. O possível impacto caso essa atualização não ocorresse dentro do previsto, poderia tornar grande, devido as seguintes dimensões, como: Confiabilidade, integridade, disponibilidade e talvez compliance.

Uma vulnerabilidade de confiabilidade pode permitir invasão dados confidenciais da empresa.

Uma vulnerabilidade de integridade pode permitir a manipulação ou danificação de sistemas e\ou dados de backup, podendo até mesmo parar a empresa.

Uma vulnerabilidade de disponibilidade caso acontecesse com sucesso, com toda certeza, deixaria sistemas inoperante e comprometendo toda a empresa.

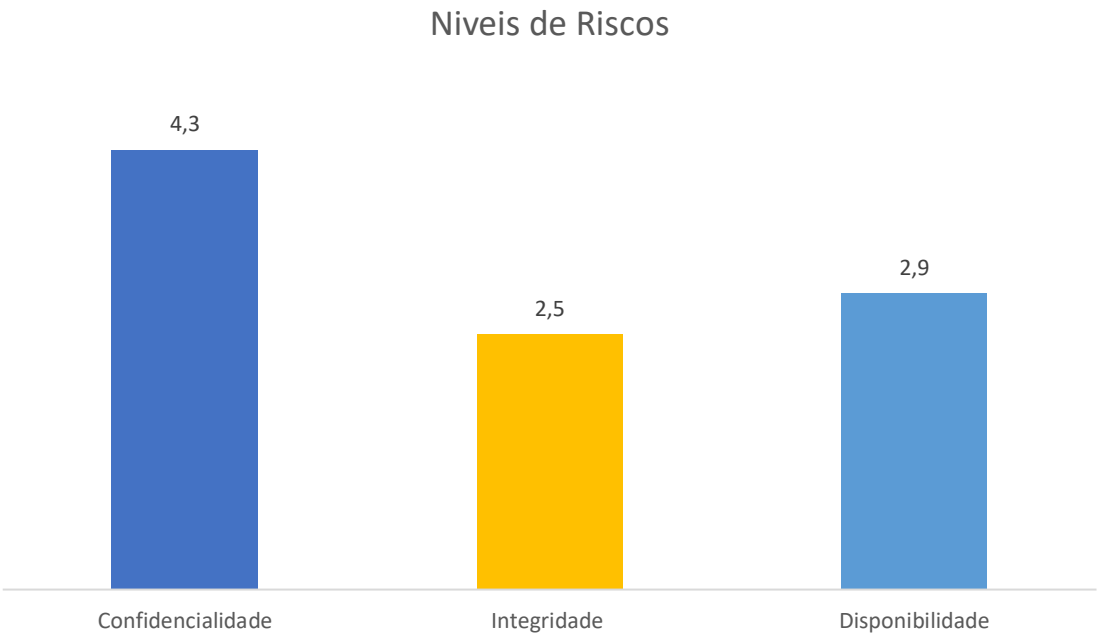
E uma vulnerabilidade de compliance, dependendo do campo requisitado, a empresa poderia enfrentar problemas para recuperar e tornar judicial o ato.

Sendo assim, precisamos entender o grau de risco exposto ao não tornar a segurança como item prioritário da empresa.

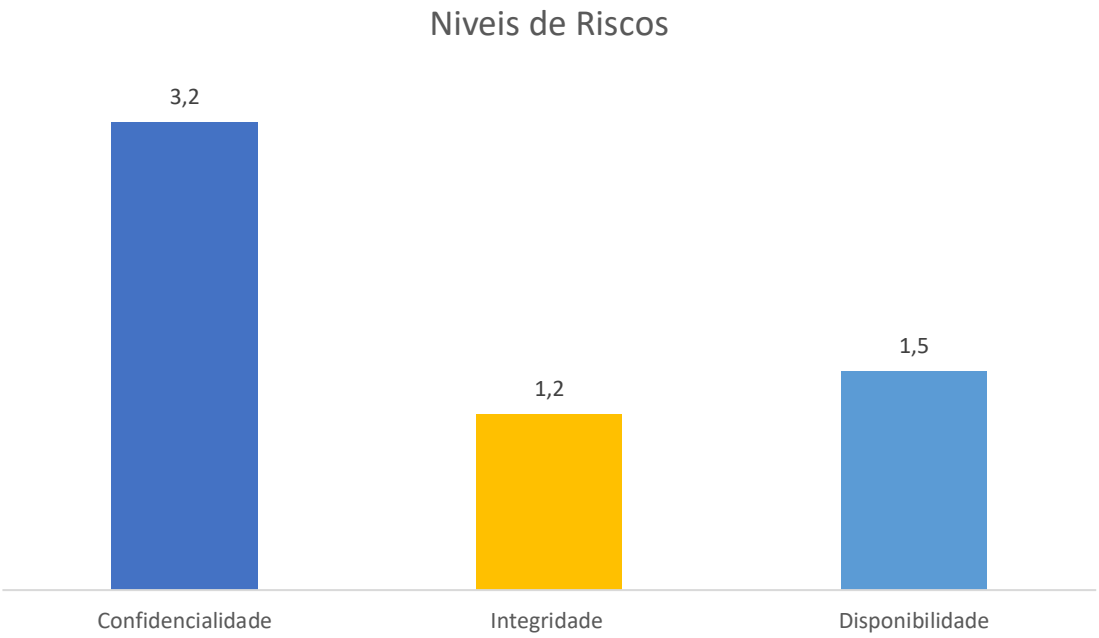
5. Relatório de avaliação

Após análise das medidas a serem implementadas, os riscos presentes na infraestrutura que foram descobertos serão quase todos mitigados definitivamente ou estarão com um percentual de risco baixo. As descobertas destes riscos foram feitas após análise minuciosa de cada parte camada da infraestrutura, desde o servidor em nuvem até o usuário final.

Os toda a análise e mitigação foram realizadas com a tríade da CID – Confidencialidade, Integridade e Disponibilidade, onde a mesma apresenta os níveis de riscos de cada ponto CID de acordo com os serviços e informações disponíveis.



Análise dos riscos antes da implementação do projeto.



Perspectiva da análise dos riscos após a implementação do projeto.

Foi utilizada uma escala de 0 a 5 para análises de vulnerabilidades onde cada ponto representa falhas no fluxo do trabalho. Após realizarmos todo o escopo do trabalho foi averiguado que o risco futuro das vulnerabilidades apresentadas terá uma queda significativa ficando um alerta no tópico de Confidencialidade que por conta de ser um indicador que está ligado diretamente com o usuário dependemos de uma boa conscientização dos usuários para garantirmos um menor grau de risco dentro da empresa.

A análise em questão levou em consideração todos os pontos de vulnerabilidades avaliados, os riscos quantitativos e qualitativos de toda o workflow dos dados desde a entrada manipulação e utilização pelos usuários internos e externos e principalmente os pontos de melhoria para mitigação dos riscos.

Para isso dividimos os tópicos e reclassificamos os mesmos assim:

- **Confidencialidade** = Medidas para evitar que terceiros acessem contas de usuários através de ferramentas MFA e atualização de todo o nosso parque de máquinas para a versão mais atual de SO, garantindo que possíveis vulnerabilidades como um ataque zero day seja explorado em nossos endpoints.
- **Integridade** = Para garantir a integridade interna e externa das informações todas as conexões internas e externas utilizarão protocolos com uma camada a mais de proteção por exemplo:
    - Conexões internas a servidores utilizarão criptografia nos acessos a servidores e bancos de dados;
    - Acessos a roteadores, firewalls e etc. Utilizarão SSH v2 para realização de acesso remoto;
    - E os acessos ao portal público da empresa será acessado apenas pela conexão 443 com o protocolo HTTPS.

- **Disponibilidade** = Para garantir a disponibilidade de todos os serviços e arquivos foi implementado o Zabbix um software de monitoramento que unifica várias ferramentas tanto para análise da infraestrutura quanto dos serviços disponibilizados.

6. Recomendações e melhorias

Com base nas vulnerabilidades identificadas e na análise de riscos, os alunos devem fornecer recomendações claras e acionáveis para melhorar a segurança da rede. As recomendações devem ser específicas, abordando cada vulnerabilidade de maneira individual e fornecendo soluções viáveis. Além disso, os alunos devem considerar o custo e a praticidade das recomendações ao propor melhorias.

Como parte da equipe de tecnologia da empresa, foram sugeridas as seguintes melhorias como:

- Atualização do sistema operacional conforme citado acima;
- Implementação de política de atualização e de segurança, e a partir daí, divulgar entre outras áreas de tecnologia;
- Ter um monitoramento mais avançado e com um olhar crítico para poder rastrear novas vulnerabilidades na rede da empresa;
- Revisão de privilégio de acesso a cada 2 meses, assim teremos uma segurança de quem pode ou não executar ações que pode ou não prejudicar a empresa;
- Treinamentos de conscientização da segurança na rede, pois assim conseguimos adotar boas práticas de segurança e conseguimos até reconhecer a ajuda do usuário para proteção da nossa empresa;
- Backups regulares dos dados da empresa, que em caso de incidente, podemos recuperar os dados atualizados a partir de um certo ponto de restauração;
- Respostas conclusivas a incidentes, pois assim desenvolvemos um plano de ação que descreve etapas a serem seguidas em caso de violação do sistema de segurança.

7. Plano de ação

Cronograma detalho:

Será realizado a partir de março 2024, com a duração de 3 semanas, tempo dedicado da equipe de segurança e TI.

Semana 1: Revisão das Configurações de Segurança

- Realizar uma reunião com a equipe de segurança para revisar as configurações do AWS WAF, Firewall Network, KMS e IAM;
- Verificar se as políticas de segurança estão alinhadas com as melhores práticas.

Semana 2: Teste de penetração e pontos fracos

- Contratar serviços de teste de penetração ou designar especialistas internos para avaliar a segurança dos endpoints;
- Analisar o impacto potencial e a probabilidade de ocorrência para cada vulnerabilidade identificada, priorizar as ações corretivas com base na análise de risco;
- Definir um plano de contingência em caso de incidentes de segurança.

Semana 3: Análise de Riscos e implantação das melhorias.

- Realizar uma análise detalhada de riscos com base nas vulnerabilidades e produzir um relatório de avaliação que inclua descobertas, análise de riscos;
- Realizaremos todas as atividades que foram sugeridas como ponto de melhorias;
- Implementar a atualização do sistema operacional para a versão mais recente;
- Estabelecer e divulgar políticas de atualização e segurança;

- Aprimorar o monitoramento para identificar novas vulnerabilidades;
- Revisar privilégios de acesso regularmente;
- Realizar treinamentos de conscientização em segurança;
- Implementar backups regulares e testes de recuperação;
- Implementar a atualização do sistema operacional para a versão mais recente;
- Estabelecer e divulgar políticas de atualização e segurança;
- Aprimorar o monitoramento para identificar novas vulnerabilidades;
- Revisar privilégios de acesso regularmente;
- Realizar treinamentos de conscientização em segurança;
- Implementar backups regulares e testes de recuperação.

Responsabilidade: Revisão das Configurações de Segurança.

- Especialistas em segurança de TI;
- Administradores de sistemas;
- Responsável pelo AWS WAF, Firewall Network, KMS e IAM;
- Testes de Penetração e Análise de Logs;
- Equipe de segurança cibernética;
- Especialistas em teste de escuridão;
- Analistas de Sistemas operacionais;
- Análise de Riscos e Produção do Relatório de Avaliação;
- Gestor de segurança;
- Implementação das Recomendações e Melhorias;
- Administradores de sistemas;
- Equipe de suporte técnico;
- Especialista em Segurança.