PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

RELATÓRIO TÉCNICO

SEGURANÇA E POLÍTICA:
REDES DE COMPUTADORES

GRUPO

Augusto Henrique Lage

Camila Ferreira Borges

Kener de Almeida Silva

Pedro Henrique Rodrigues da Silva

Sergio de Oliveira Bernardes Nunes

Raynan Rainer Ferreira de Almeida

2023

SUMÁRIO

LISTA DE FIGURAS

LISTA DE GRÁFICOS

1 INTRODUÇÃO

Neste documento serão abordados vários assuntos relacionados a melhoria contínua, otimização do ambiente de infraestrutura, possibilidade de upgrades e adesões de novos equipamentos ou serviços e a consolidação de infraestrutura recentemente implementada.

2 REVISÃO DAS MEDIDAS DE SEGURANÇA IMPLEMENTADAS

Durante a implementação da infraestrutura na CECC, nós nos programamos para tratar a implementação do firewall de forma majoritariamente restritiva, ou seja, tudo é bloqueado exceto o que liberamos. Sendo assim, em relação ao firewall até este momento está dentro dos conformes e as liberações futuras acontecerão de acordo com que as necessidades da empresa respeitando a política de segurança e passando pelo crivo da diretoria e responsáveis pela infra.

No andamento da revisão percebemos algumas necessidades pendentes para a infraestrutura da CECC, as quais entrarão como melhoria de serviço que são estes:

1. Monitoramento de Ativos com Zabbix Server.
2. Adicionar Nobreak com mais autonomia
3. Controle de Acesso ao CPD

2.1 Pontos Fortes

Ao revisar toda infra implementada, podemos destacar alguns pontos fortes que conseguimos implementar na empresa, assim como alguns pontos de melhoria futura.

Quanto aos pontos fortes destacaremos os itens apontados abaixo:

2.1.1 Gestão de usuários centralizada

Antes de implementarmos o servidor de autenticação Active Directory, os colaboradores utilizavam usuários locais nas estações, o que dificultava o gerenciamento uma vez que para cada estação o usuário precisava ser recriado. A gestão com Windows ADDS facilita a gestão do administrador de TI e ainda possibilita vários tipos de integração com outros sistemas.

2.1.2 Políticas de troca de senhas e configurações de uso comum

Com este mesmo serviço, também ganhamos a possibilidade de criar políticas de grupo. Tal funcionalidade nos permite criar alguns padrões para que toda estação ou usuário herde as configurações que são impostas, não podendo ser alteradas por usuário final. Alguns exemplos são:

- Padronização de papel de parede;
- Mensagem de boas-vindas;
- Mapeamento automático de drive de rede e impressora;
- Política de troca de senhas com padrões especificados pelo Administrador de TI;
- Definir página inicial da empresa nos navegadores.
- Configuração automática de proxy nas estações

Estes são apenas alguns exemplos do que implementamos. As diretivas de grupo nos auxiliam na gestão do ambiente corporativo, impondo, restringindo ou até mesmo liberando certos recursos de forma granular, claro, isso exige certo nível de conhecimento.

2.1.3 Controle de acesso aos arquivos baseado em nível permissões

Como já mencionado no projeto, o servidor de arquivos foi uma das grandes melhorias e ponto forte adquirido pela empresa. Pois, é através destes serviços que conseguimos fazer todo o controle do que: "**Quem pode acessar o quê?".** O Servidor de arquivos trabalha diretamente com o ADDS, pois, graças a ele, podemos controlar as permissões através de grupos que criamos no Active Directory, então, caso um usuário não faça parte de nenhum grupo não terá acesso a nada, mesmo que ele já esteja criado no domínio.

2.1.4 Firewall com Web Proxy e controle de acesso Web com interceptação SSL

Uma das melhores implementações que fizemos na CECC, certamente foi o firewall. Antes, não havia controle de nada, tudo era liberado e qualquer coisa poderia ser acessada na internet, o que é um risco enorme para qualquer empresa. Hoje, com o firewall nós conseguimos trabalhar de forma mais efetiva, controlando o fluxo das informações, já que nosso firewall está configurado para bloquear qualquer coisa que não é permitido. É por ele que conseguimos fazer o controle de internet, os bloqueios de sites que podem tirar a produtividade do colaborador, através do Web Proxy. Ele também nos entrega relatórios de acesso web por usuário.

2.1.5 Controle de web baseado em grupos e integrado ao Active Directory

Ainda engajado no firewall, a aplicação nos deu um leque de opções. Já que, conseguimos fazer várias integrações com o ADDS, o firewall não seria diferente. Quando integramos o Firewall com o ADDS, conseguimos criar os perfis de acesso em níveis diferente, garantindo que os usuários tenham o acesso web de acordo com o setor.

2.1.6 Redundância de Links de internet e Failover

No Firewall conseguimos configurar as duas funções para garantir a redundância dos links de internet. Além de configuramos um failover o que nos garante que, se o link principal de internet cair, o secundário entra em ação para suprir a demanda até que o link principal se restabeleça. Isso é feito de forma automática a partir do mento que apontamos a priorização dos links no firewall.

Já o balanceamento nos permite utilizar de o link secundário ao mesmo tempo que o primário, uma vez que no failover ele fica ocioso.

2.1.7 Relatórios de acesso Web

O firewall ainda nos dá acesso à relatórios web. Essa parte do firewall é de extrema importância, pois ele nos ajudará em vários aspectos, como melhoria contínua e possíveis auditorias. O relatório em questão, vem com informações de data, hora, usuário e site acessado. Podemos acessar um dia e ano específico de acordo com o tempo de retenção dos logs.

2.1.8 Backup periódicos

Além de ferramentas de autenticação, segurança de borda e controle de acesso, contamos ainda com um servidor de backup utilizando a ferramenta Veeam backup, que é gratuita para até 10 instâncias. Para garantir um backup ainda mais eficiente, além do backup local que é feito em um storage que é usado como armazenamento no Veeam, após o backup local, também adicionamos um schedule para enviar uma cópia deste backup para um provedor cloud para garantir uma recuperação em caso de Disaster Recovery.

2.1.9 Antivírus

Não menos importante, garantimos um servidor de antivírus com um end point para adicionarmos mais uma camada de segurança. A vantagem deste tipo de serviço, é que, as atualizações são diárias e são baixadas diretamente do servidor local da aplicação que retem as atualizações. Em horário agendado previamente na console de administração do EndPoint configuramos a distribuição para as estações que se comunica através de um agente. Isso garante economia de banda e gestão centralizada da saúde cibernética das estações.

2.2 Vulnerabilidades e Pontos Fracos

2.2.1 Firewall Open Source: Limitação de listas de Web Filter

Embora a internet seja cheia de documentação do firewall pfSense, ele é um firewall que depende da comunidade. Não que isso seja, ruim. Mas, muitas features hoje em dia no mercado, o pfSense não oferece. Se formos honestos e fizemos uma comparação entre um firewall UTM e NGFW, não haverá o que ser discutido.

Não que seja um ponto fraco, mas, o web proxy hoje, para que possamos configurar e categorizar acessos, nós utilizamos uma lista que anteriormente era mantida por um desenvolvedor da comunidade; A Shallalist que infelizmente foi descontinuada. A Shallalist, é uma lista de sites categorizados que pode ser usada para fazer o controle de acesso de conteúdo web. Embora a o desenvolvedor tenha descontinuado o belo trabalho, a lista ainda é muito utilizada. Existem outras listas, porém, como é algo que depende de a comunidade desenvolver acaba gerando essa brecha. Imagine ter que bloquear site por site, todos os dias na unha, seria um trabalho muito moroso e geraria um esforço administrativo tremendo.

2.2.2 Ausência de um host secundário para replicação da infra atual

O maior ponto fraco que podemos encontrar na atual infra, é a falta de um servidor secundário, este que faria por sua vez, faria o papel de um failover total dos servidores, como utilizamos o Microsoft Hyper-V, com um servidor secundários poderíamos replicar o ambiente que hoje está em produção para o servidor secundário a cada 15 minutos, sendo assim, em caso de falhas de hardware no servidor primário, bastaria ligar as vms no servidor secundário e o máximo que informação que perderíamos, seriam dos 15 minutos passados após a última replicação, impactando minimamente o ambiente de produção.

2.2.3 Controle de Acesso ao CPD e Energia

O controle de entrada e saída do CPD foi algo que também notamos que precisaríamos mudar ou, sugerir a mudança. Adicionar um método de leitura de biometria, ou cartão eletrônico para acesso à central de processador de dados é algo crucial para qualquer empresa, uma vez, que, as informações que estão ali, são as fontes de produção de todo o time. Um acesso indevido, pode trazer sérios prejuízos a qualquer empresa; neste cenário, ainda não temos um servidor secundário para garantir uma redundância de ambiente. Ainda podemos encontrar no ambiente a falta de um nobreak mais adequado à nova realidade, como o servidor atual possui duas fontes para redundância é necessário que a empresa garanta energia o suficiente para que não ocorram danos por falta de energia ou quedas inesperadas.

Dentro do que está sendo mencionado, fizemos uma matriz de risco. Embora básica, ela nos permitirá mensurar quais os possíveis efeitos e chances temos de enfrentar certos problemas que podem acontecer em qualquer empresa. Nos dará também, a possibilidade de ciar um plano de ação para tratar estes problemas.

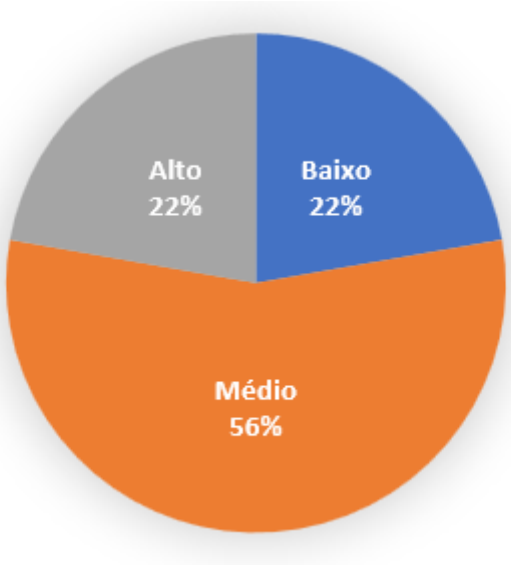
Matriz de risco – Básica

Matriz de Risco - CECC										
Itens	Risco	Impacto	Setor	Efeito	Ação recomendada	Plano de ação	Data da Aprovação	Data de início	Data de término prevista	Data Limite
Links de internet	1	Médio	Conectividade	Pode haver lentidão da internet dependendo do link que cair	Entrar em contato com provedor de internet	Considerado médio por ter dois links de internet	-	-	-	-
Firewall	2	Alto	Infraestrutura	Parada total do serviços de rede	Em caso de falha de software tentar tentar fazer restauração do backup Em caso de falha de hardware acionar a garantia do equipamento	Subir o novo firewall e restaurar as configurações do backup anterior	20/12/2023	01/08/2024	31/12/2024	03/02/2025
Switchs	2	Alto	Infraestrutura	Parada total ou até parcial para estações de rede, impressoras e acess points	Garantir ao menos um switch para possível reposição	Substituir ou compra de um novo switch	20/12/2023	05/02/2024	22/04/2023	30/04/2023
Servidor	2	Alto	Infraestrutura	Para total do serviços	Em caso de falha de software tentar tentar fazer restauração Em caso de falha de hardware acionar o suporte do fornecedor	Garantir hardware igual ou superior para serviço de replica da infraestrurura existente	20/12/2023	03/06/2024	31/12/2024	03/02/2025
Estações	2	Médio	Produtividade	Para parcial da estação	Verificar o hardware e fazer o check do equipamento	Efetuar o check inicial e sendo constatado defeito de hardware acionar a garantia do equipamento	-	-	-	-
Acess points	1	Baixo	Conectividade	Possível parada parcial da rede wireless em alguns pontos	Verificar o hardware e fazer o check do equipamento	Efetuar o check inicial e sendo constatado defeito de hardware acionar a garantia do equipamento	-	-	-	-
Fornecimento de Energia	3	Alto	Energia	Para total do serviços	Entrar em contato com o fornecedor de energia local	Verificar a possbilidade de instalação de gerador de	20/12/2023	05/02/2024	03/06/2024	01/07/2024
Refrigeração do CPD	2	Médio	Energia	Sobreaquecimento nos equipamento e possível lentidão na rede dados	Acionar o departamento de manutenção responsavel	Acionando o setor responsável pela manutenção e fazer o acompanhamento do reparo do mesmo	-	-	-	-
Controle de acesso ao CPD	3	Alto	Infraestrutura	Um acesso indevido por causar danos permanentes	Fazer controle diário de acesso ao CPD	Implementar uma forma mais segura de controle de acesso.	20/12/2023	05/02/2024	23/02/2024	29/02/2024

Fonte: Plano de Ação.xlsx

Trazendo essas informações para melhor compressão, podemos analisar os gráficos abaixo onde classificamos em graus de risco, sendo eles: Baixo, Médio e Alto.

Gráfico 1 - Grau de risco por categoria

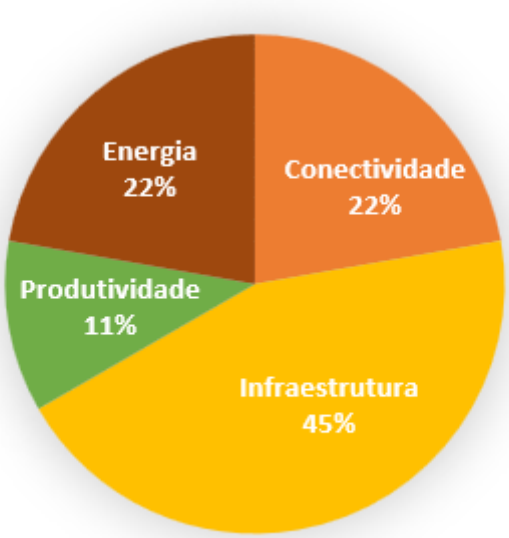


Fonte: O autor

Neste cenário, avaliamos as chances de cada item avaliado acontecer. Então, temos o GAP de mais de 50% para ser tratado, este número está relacionado ao maior gargalo que encontramos durante a revisão das implementações, que é o fator energia.

Já quando fazemos a avaliação de impacto direto por setores, podemos verificar que os setores mais afetados são os de infraestrutura, com 45% da projeção do impacto, embora a energia esteja com 22% neste gráfico, vimos que no anterior é o principal ponto de falha, pois que a energia ficar indisponível, toda a operação fica parada. Os 45%, são primeiras coisas a serem afetadas, pois em caso de uma queda brusca de energia, além e afetar a produtividade como um todo, os danos causados por quedas inesperadas podem ser severos, causando danos tanto no funcionamento do software quanto do hardware.

Gráfico 2 - Grau de risco por Setor



Fonte: O autor

2.2.4 Monitoramento e Câmeras de Segurança

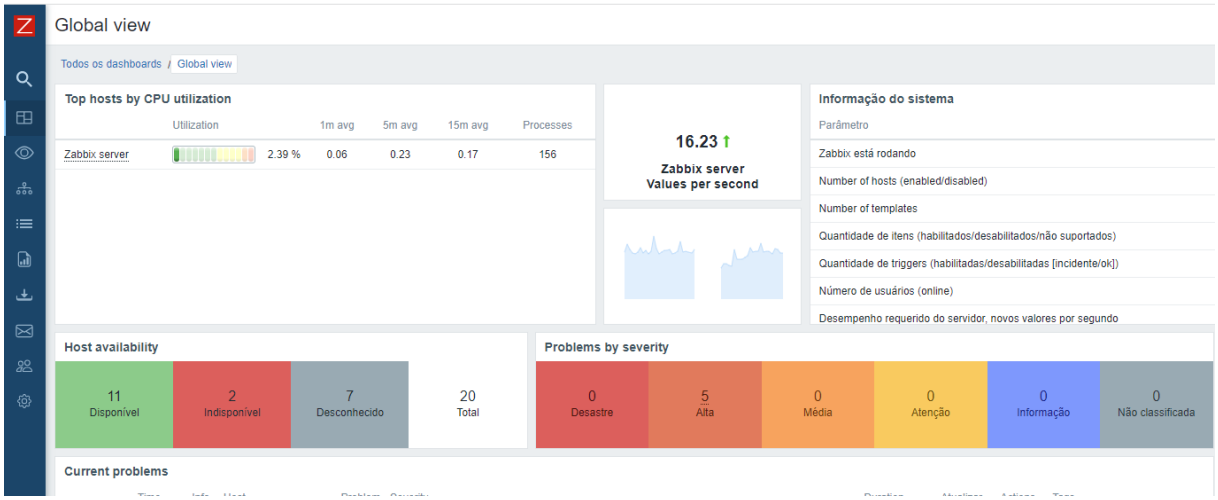
Neste tópico abordaremos um pouco da ferramenta Zabbix e CFTV, a qual implementamos como ferramentas adicionais para monitorar os links de internet e os ativos de rede, bem como a segurança de tráfego de pessoal dentro da CECC. Assim, podemos acompanhar a saúde dos equipamentos da empresa e manter a vigilância no ambiente empresarial.

Foram instaladas algumas câmeras ip nas instalações da CECC visando garantir a segurança e integridade física dos colaboradores e alunos. As imagens serão armazenadas por um período de 30 dias, as filmagens foram configuradas para filmar 24 horas por dia em um NVR Intelbras.

Quanto a implementação do serviço de monitoramento de rede, adicionamos mais uma máquina virtual com o sistema operacional Linux Debian, onde instalamos o serviço do Zabbix.

Configuramos para monitorar os ativos de rede, os switches, as VMs e os servidores host. É no Zabbix que conseguimos alguns parâmetros importantes, como por exemplo saber a demanda de recursos para os servidores. Com as triggers configuraras, saberemos quando o servidor está tendo uma demanda acima do que era esperado, bem com saber quando um servidor não está utilizando todo o recurso alocado para ele. Isso nos permite ir otimizando o ambiente até chegar em um ponto que temos um funcionamento ser qualquer tipo de gargalos.

Figura 1 - Dashboard Inicial do Zabbix



Fonte: o autor

2.3 Recomendação de melhorias

2.3.1 Energia

Uma vez feito toda a análise com a matriz onde fizemos os checks da nova infra e que inclusive já foram apontados alguns planos de ações que devem ser considerados. Abordaremos os fatores que fizeram com que esses planos fossem abertos.

Como já mencionado, o problema mais crítico é o fator energia. Hoje, a CECC conta apenas com o fornecedor de energia local, embora as empresas de energia tenham um SLA dentro de padrões estabelecidos pelos órgãos competentes. É importante que a empresa entenda por completo o cenário em que ela está inserida. Uma vez identificado que o maior ponto de falha é falta de energia, devemos pensar em um plano de contingência para sanar o problema até que tudo se normalize. A implementação de um gerador tem um investimento considerável, entretanto, é um investimento que garantirá a continuidade do negócio.

Ainda falando sobre energia, um ponto chave identificado dessa revisão, foi a falta do nobreak dentro do CPD, para que os ativos de rede continuem funcionando sem sofrer nenhum impacto de forças externas. A adição de um nobreak para estes equipamentos é algo que precisa ser feito com certa urgência, uma vez que, não há um hardware secundário para substituição dos que hoje estão em produção.

2.3.2 Hardware Secundário

Na implementação, embora todos os servidores sejam virtualizados, temos a elo fraco nessa infra quanto se trata de hardware. Assim como no gerador, um servidor secundário também tem um custo considerável, mas, também passa ser um item crítico de ponto de falhas. Se um servidor que estar virtualizado falhar, tudo bem, apenas restauramos o backup e o impacto é baixo. Mas, a história é diferente se o servidor host falhar, sendo que, todos os serviços com exceção do firewall estão embarcados nele. Então, um servidor secundário com configurações iguais ou até mesmo superior, é importante para que seja feito um cluster de failover, ou um serviço de réplica para garantir o SLA interno mínimo.

2.3.4 Firewall Implementação de QoS

O pfSense é um firewall usado em todo e com comunidade em todo o mundo. Porém, é um firewall UTM de código aberto como mencionado anteriormente e é sustentando pela comunidade. Uma das melhorias que consideramos importantes é a substituição do pfSense por um outro firewall NGFW, como as soluções da Fortinet por exemplo. Diferente do pfSense, a Fortinet tem equipes prontas para atualizar as listas de web filter entre outras definições do sistema; os equipamentos licenciados recebem as atualizações todos os dias mantendo uma base de dados segura e atualizada. Outro fato importante que sugerimos como melhoria é a implementação de o QoS (Quality of Service) para garantir uma melhor aderência no negócio, priorizando o tráfego que é pertinente a CCEC.

2.3.5 Treinamentos e aplicação das Políticas de Segurança da informação

Por fim, um dos pilares mais importantes são colaboradores treinados e vacinados quanto ao comportamento na frente de uma tela, seja de um computador ou smartphone. O treinamento contínuo dos colaboradores ajuda na educação com a cyber segurança, pois, grande parte dos usuários, não tem ideia do que é engenharia social, malware ou um ransonware. Então, a partir do momento que temos um time nivelado com um mesmo pensamento crítico quando a segurança da informação, conseguimos manter uma consistência na segurança da informação no local de trabalho. Uma equipe bem-informada e engajada com o negócio é o pilar da uma instituição. Por mais que a rede esteja o trabalhando de forma mais restritiva, nenhuma rede está 100% protegida, então, se temos os equipamentos e nossa rede lógica bem configurada, nos resta investir no fato humano, que é a parte intelectual e comportamental da empresa, o que

no caso da CECC, envolve uma mudança de cultura, uma vez que na estrutura anterior eles tinham acesso irrestrito a qualquer tipo de conteúdo.

3 CONSIDERAÇÕES FINAIS

A partir dos resultados informados nesse relatório técnico, concluímos a revisão das medidas de segurança implementadas as quais foram definidas ressaltando: Monitoramento de Ativos com Zabbix Server, adição Nobreak e fortalecimento do Controle de Acesso ao Centro de Processamento de Dados. A identificação de pontos fortes e fracos são imprescindíveis respectivamente pois, dominar e reconhecer situações que podem ou não ser adversas, transformam em oportunidades para a evolução da empresa e consequentemente, não torne um novo obstáculo.

Contudo, a partir da aprovação desse relatório de melhorias será iniciado o programa de implantação dos itens de melhoria mencionados na tabela: “Matriz de risco – Básica”. O cronograma de implantação seguirá a ordem de maior item de criticidade para o menor, na tabela informada também contém as datas da previsão de início e término da implantação.

Assim sendo, o prazo limite de aprovação desse relatório deverá ser até 20 de dezembro de 2023. Os processos de maior criticidade estão previstos para iniciar a partir de fevereiro de 2024, exceto o Firewall e o Servidor Secundário que possuem previsão para iniciar em agosto de 2024, com previsão de término em dezembro de 2024, podendo sofrer alterações no prazo, por se tratar de itens com o custo elevado e estarem na garantia do fornecedor. O investimento mais pesado, é o gerador de energia, que resultará em várias soluções simultâneas, uma vez que o gargalo da energia provoca o maior impacto no plano de ação. Com data de início para 05 de fevereiro de 2024 e com previsão de término em 03 de junho de 2024 também podendo sofrer alterações no prazo. Enfim, temos o Controle de Acesso ao CPD e Switchs para previsão de término respectivamente para 23 de fevereiro de 2024 e 22 de abril de 2024, ambos podendo sofrer alterações no prazo. Em simultâneo com a correção dos itens sinalizados, conseguiremos corrigir os demais no mesmo prazo.