PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Projeto apresentado no Eixo 5 do curso superior de Tecnologia em Redes de Computadores

Orientador: Prof: Luiz Ferreira

Sumário

1. INTRODUÇÃO

Com o crescente panorama da tecnologia da informação e a dependência cada vez maior das organizações em relação a sistemas de redes, a segurança da informação se tornou uma prioridade crucial.

Neste relatório, é realizada uma avaliação abrangente das medidas de segurança implementadas na rede de informações pelo Grupo 03. O objetivo desta avaliação é identificar pontos fortes, vulnerabilidades e recomendar melhorias para garantir a conformidade com os requisitos de segurança estabelecidos, bem como para fortalecer a postura de segurança da rede de informações.

A análise é conduzida com base em uma revisão minuciosa das medidas de segurança existentes, uma identificação detalhada de pontos fortes e vulnerabilidades, uma análise de riscos e recomendações práticas para aprimorar a segurança geral da rede.

Este relatório oferece insights valiosos para a otimização contínua da segurança de informações e infraestrutura de rede do Grupo 03, com o objetivo final de fortalecer a resiliência contra ameaças cada vez mais sofisticadas e emergentes no cenário atual de segurança cibernética.

2. APRESENTAÇÃO

O relatório de avaliação de segurança da rede de informações apresenta uma análise detalhada das medidas de segurança implementadas na rede. O objetivo central deste relatório é identificar pontos fortes e vulnerabilidades na rede, proporcionando uma visão abrangente das áreas que requerem melhorias para garantir a conformidade com os padrões de segurança estabelecidos.

Inicia-se com uma revisão das medidas de segurança atuais, abrangendo firewalls, controle de acesso, criptografia e monitoramento. Em seguida, são destacados os pontos fortes da rede em termos de segurança, seguido de uma análise aprofundada das vulnerabilidades e pontos fracos identificados.

Com base nessa análise, uma avaliação de riscos é realizada, ajudando a priorizar ações corretivas e a determinar as medidas de segurança que devem ser implementadas ou aprimoradas. O relatório também fornece recomendações práticas e acionáveis para melhorar a segurança da rede, levando em consideração o custo e a viabilidade das soluções propostas.

Finalmente, um plano de ação é apresentado, delineando as etapas necessárias para a implementação das recomendações de segurança propostas. Este relatório visa fortalecer a resiliência da contra ameaças cada vez mais sofisticadas no cenário atual de segurança cibernética em constante evolução.

3. OBJETIVO

O objetivo primordial deste relatório é realizar uma análise abrangente das medidas de segurança atualmente implementadas na rede de informações criado pelo Grupo 03. Através dessa avaliação, pretende-se identificar tanto os aspectos sólidos quanto as fragilidades existentes, fornecendo recomendações práticas e acionáveis para fortalecer a postura de segurança da rede e assegurar o cumprimento dos padrões de segurança estabelecidos.

Este relatório busca oferecer insights significativos para orientar a implementação de estratégias eficazes, visando reforçar a adequação da rede diante de ameaças cibernéticas cada vez mais complexas. Além disso, visa proporcionar um plano de ação detalhado que oriente a implementação das melhorias propostas para a segurança da rede de dados e informações.

4. REVISÃO DAS MEDIDAS DE SEGURANÇA

Nós do grupo03, adotamos algumas medidas de segurança, e as utilizadas como pilares fundamentais para estruturação de segurança da rede. Não nos restringimos em seguir apenas essas diretrizes, mas as utilizando como pilares fundamenteis para estruturação da segurança da rede.

Primeiro ponto foi a criação de credenciais nominais exclusivas para os responsáveis gerenciarem os servidores, com políticas de senhas mais agressivas. Realizamos a segmentação da rede com VLANS,, de acordo com cada setor, aumentando o nível de segurança e gerenciamento da rede.

No firewall foram parametrizadas apenas regras necessárias para o operacional. O acesso às dependências físicas internas é restrito e devidamente controlado.

Visitantes só podem transitar pelas dependências da empresa com aprovação e acompanhamento de algum gestor, mediante apresentação de documentos na portaria e utilização de crachá de visitantes. Todo acesso a equipamentos ou serviços devem passar previamente pela Gestão de Infraestrutura, e somente ela aprovará e tratar se é cabível a liberação.

5. IDENTIFICAÇÃO DE PONTOS FORTES

Revisando todos os itens implementados, podemos apontar vários pontos fortes.

- Segmentação de rede por Vlans, protegendo a rede de ataques cibernéticos, restringindo o acesso a ativos críticos e impedindo que uma ameaça se espalhe por toda a rede.

- Firewall com IDS/IPS, auxiliando na detecção e bloqueio de ataques, fortalecendo a segurança da rede. Além de constantes revisões nas regras existentes, mantendo apenas regras realmente necessárias e que não comprometam a integridade da infraestrutura.

- File-Server devidamente estruturado, com políticas de acesso aos arquivos com base em grupos de usuários do Active Directory, garantindo assim que, nenhum colaborador tenha acesso a arquivos de forma indevida, diminuindo a possibilidade de vazamento das informações sigilosas de cada área e setor.

- Implantação de um certificado SSL no servidor web, fornecendo uma camada adicional de segurança e confiabilidade, o que é essencial para proteger os acessos.

Rotinas mensais para aplicação de patchs de segurança em servidores Windows e Linux, pois são essenciais para proteger os sistemas e dados de uma empresa contra-ataques cibernéticos e trazerem melhorias aos sistemas com as últimas versões de softwares.

- Realização de treinamentos, palestras e e-mails sobre segurança da informação, consolidando como medidas eficazes para conscientização dos colaboradores, sobre os riscos e como evitá-los. Auxiliando na criação de uma cultura de segurança dentro da empresa, tornando os colaboradores mais conscientes das ameaças e mais propensos a tomar medidas para se protegerem.

6. IDENTIFICAÇÃO DE VULNERALIBIDADE E PONTOS FRACOS

Os pontos de atenção que devemos ficar atentos em uma estrutura de rede, podem surgir de várias fontes, desde falhas de segurança em software e sistemas operacionais até falhas físicas. Esses dependem de manutenção rigorosas, a fim de mitigar qualquer possibilidade de falhas causadas por falhas inerentes de operação ou interoperabilidade.

Em se tratando de um ambiente on primisse, existe a dependência de uma única concessionaria de energia. Há o risco de incêndio, devido a alguns produtos na estrutura da empresa serem altamente inflamados. Esses eventos podem causar perda de dados ou interrupção dos serviços. Temos também a dependência de um único link de internet, aumentando o risco de indisponibilidade dos serviços. Além de não possuirmos redundância para o serviço de File Server, Active Directory, Firewall e link de internet, incluímos entretanto, alguns pontos críticos para melhorias urgentes.

7. ANÁLISE DE RISCO

A análise de riscos é uma etapa fundamental para garantir a segurança e proteção das informações em uma organização. Para isso, é importante utilizar metodologias reconhecidas internacionalmente, como a ISO-31000 e a ISO-27001.

7.1. ISO-31000

É uma norma que estabelece princípios e diretrizes para a gestão de riscos. Ela fornece um processo sistemático e estruturado para identificar, analisar e avaliar os riscos, permitindo que a organização tome decisões informadas sobre como lidar com eles.

7.2. ISO-27001

É uma norma específica para a gestão da segurança da informação. Ela estabelece requisitos para a implementação de um sistema de gestão de segurança da informação, incluindo a análise de riscos como parte integrante desse sistema.

Utilizando estas normas como referências, bem como frameworks podemos atuar para:

- Identificar riscos relacionados à segurança da informação (riscos cibernéticos).
- Escolher um item para aplicar Análise de Riscos, com base no contexto atualizado do ambiente interno, objetivo do nosso trabalho.
- Realizar a Avaliação do risco escolhido, classificando seu impacto, probabilidade e conseguinte nível de risco.
- Identificar vulnerabilidades e medidas recomendadas para atenuá-las.

No contexto da gestão de riscos em ambientes de rede, a eficácia na mitigação de ameaças exige a instituição de processos de gestão de configuração extremamente robustos. Além disso, é crucial conduzir auditorias sistemáticas

periódicas, garantir a aplicação diligente de atualizações e patches, e proporcionar treinamento contínuos para os administradores de rede e usuários comuns.

Este escopo abrange elementos críticos, incluindo a manutenção dos ativos da estrutura de rede, como; firewall, a gestão do Active Directory, a adequação de permissões de usuários, e a execução de rotinas de controle para todo o ambiente de Tecnologia da Informação (TI). Paralelamente, é fundamental a implementação de um plano de respostas a incidentes críticos, capacitando uma resposta ágil e eficiente diante de potenciais violações de segurança.

8. DIFINIÇÕES

8.1. Risco

É efeito da incerteza nos objetivos. Um efeito é um desvio em relação ao esperado. Pode ser positivo, negativo ou ambos, e pode abordar, criar ou resultar em oportunidades e ameaças. Risco é normalmente expresso em termos de fontes de risco, eventos potenciais, suas consequências e suas probabilidades.

8.2. Risco Inerente (Bruto)

Risco intrínseco ao negócio ou à atividade da Organização, sem considerar a execução de controles e ações para tratar sua exposição, também chamado de risco bruto.

8.3. Probabilidade

Chance de algo acontecer ou possibilidade de um risco ocorrer. Isso pode ser expresso em termos de ocorrência de uma probabilidade ou frequência.

8.4. Agravantes

Vulnerabilidades, fatores ou causas que aumentem a probabilidade do risco se materializar.

8.5. Impacto

Resultado ou efeito de um risco, considerando os controles corretivos existentes para mitigá-lo. O impacto de um risco pode ser positivo ou negativo em relação

à estratégia ou aos objetivos. Também denominado de severidade/criticidade para riscos operacionais ou ocupacionais.

8.6. Atenuantes

Medidas, controles ou ações que tem o potencial de impedir a materialização do risco ou atenuar seu impacto no caso de ocorrência.

8.7. Nível de Risco

Magnitude de um risco resultante da combinação dos fatores de probabilidade e impacto.

8.8. Gestão de Riscos

Gerenciamento de riscos corporativos composto por estrutura, princípios e processo conduzido pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias e formulado para:

8.8.1. Identificação

Identificar em toda a organização eventos em potencial, capazes de afetá-la

8.8.2. Administração

Administrar os riscos de modo a mantê-los compatíveis com o apetite de risco;

8.8.3. Possibilidade

Possibilitar garantia satisfatória do cumprimento dos seus objetivos.

9. IDENTIFICAÇÃO

O gerenciamento de riscos corporativos abrange pilares e categorias para distinguir a natureza dos riscos organizacionais e suas respectivas estratégias de tratamento, como por exemplo, riscos estratégicos, financeiros, riscos operacionais, de saúde e segurança, riscos legais, riscos de compliance etc.

9.1. Riscos Cibernéticos

Eventos que podem expor os ativos de informação, afetar a confidencialidade das informações e comprometer a integridade e disponibilidade de dados ou sistemas tecnológicos da Companhia.

9.2. Análise do Ambiente Interno

Refere-se à tentativa de destruir, expor, alterar, desativar, roubar, obter acesso não autorizado de um ativo da infraestrutura de rede.

10. CONSEQUÊNCIAS

I - Indisponibilidade dos ambientes corporativos, financeiro, sistemas e ferramentas de comunicações.

II - Vazamento de informações estratégicas e confidencias ao negócio, bem como dados sensíveis dos funcionários, fornecedores e cliente.

10.1. Possibilidades

I - Elevado número de tentativas de invasões.

II - Ausência de monitoramento de ameaças contemplando todos os ativos do ambiente.

III - Vulnerabilidade na proteção de dados dos clientes internos (LGPD).

IV - Ausência de investimento em segurança da informação

V - Equipe de segurança da informação reduzida.

VI - Acúmulo de funções no time de TI

10.2. Tratativas

I - Firewall: Proteção de perímetro para entrada e saída de internet em todo o ambiente de rede.

II - WAF (Web Application Firewall): Proteção contra-ataques a todos sistemas e sites públicos para internet.

III - Anti-Spam: Proteção contra ameaças que podem se disseminar por e-mails.

IV - Data Center migrado 100% para AWS. (Atualmente está híbrido com alguns serviços on-primesses e nuvem)

V - Seguro para cobrir riscos cibernéticos

VI - Utilização de soluções da gestão de vulnerabilidades e Gestão de Atualizações (Patchs de segurança, nuvens e System Center)

11. OBJETIVO DO INDICADOR DE RISCO

Aplicar, corrigir e monitorar as vulnerabilidades e atualizações em aderencia as ferramentas e estratégias em Cyber Security, definidas pelo Grupo 03.

I - Apurar o volume de ofensas e ataques monitorados pela plataforma SIEM.
II - Apurar as vulnerabilidades identificadas no período, identificadas através da plataforma de gestão de vulnerabilidades.
III - Classificar as vulnerabilidades de acordo com o nível de criticidade: crítica, alta, leve e baixa.

12. RECOMENDAÇÕES

- Realizar investimentos em segurança da informação: Destinar recursos financeiros para aquisição de ferramentas e tecnologias de segurança, como soluções de prevenção de intrusões, detecção de malware e autenticação multifator.

- Realizar treinamentos e conscientização em segurança da informação: capacitar os colaboradores para identificar e evitar possíveis ameaças, como phishing e engenharia social.

- Realizar testes de penetração e avaliações de vulnerabilidades: identificar e corrigir possíveis falhas de segurança antes que sejam exploradas por atacantes.

- Revisar e atualizar regularmente as políticas e procedimentos de segurança da informação: garantir que as diretrizes estejam alinhadas com as melhores práticas e que sejam revisadas e atualizadas conforme necessário.

Ao implementar essas medidas em ordem de prioridade, O grupo 03 fortalecerá sua postura de segurança da informação e reduzirá os riscos de um ataque cibernético. É importante ressaltar que a segurança da informação é um processo contínuo e que deve ser revisado e atualizado regularmente para se adaptar às novas ameaças e vulnerabilidades.

13. PRODUÇÃO DE RELATÓRIO DE AVALIAÇÃO

Um relatório de avaliação de segurança de redes e informações deve ser claro, abrangente e orientado para ação. A avaliação de segurança de redes e informações é uma parte vital da estratégia de proteção contra ameaças cibernéticas. Um relatório deve buscar apresentar uma visão abrangente do estado atual da segurança, identificando vulnerabilidades, destacando áreas de excelência e fornecendo recomendações para fortalecer as defesas cibernéticas da organização.

Dentre os resultados que podem ser apresentados na avaliação, podemos citar, o levantamento do número de vulnerabilidades e a classificação de acordo com sua gravidade para que seja feita a ordem de prioridade para correção, dados que demostre a efetividade das medidas de segurança já existentes e recomendações que evidencie os pontos que carecem de mais atenção, e melhorias para atender aos requisitos emergentes.

Um relatório de avaliação destaca a importância contínua da segurança de redes e informações. Ao abordar as fragilidades identificadas e implementar as recomendações fornecidas, a organização estará mais bem preparada para enfrentar os desafios cibernéticos emergentes, fortalecendo assim sua resiliência digital e protegendo seus ativos de informação. Vale lembrar também, que a partir de um relatório é possível aperfeiçoar os treinamentos e enriquecer as orientações para os usuários, de forma a conscientizar dos cuidados e práticas que corroboram para o cultivo de uma rede segura.

14. RECOMENDAÇÕES E MELHORIAS

Após auditoria, visando manter o ambiente em compliance, destacamos os itens que precisam ser implementados.

14.1. Inclusão AD

Inclusão de um servidor Windows Server 2022 com função de Active Directory secundário, garantindo que os colaboradores possam continuar a acessar recursos de rede mesmo se o servidor primário estiver indisponível. Melhorando o desempenho ao distribuir a carga de autenticação e autorização entre os dois servidores, além de manter uma cópia redundante do banco de dados do Active Directory, ajudando a proteger os dados contra perdas ou danos.

14.2. Inclusão File Server

Inclusão de um servidor Windows Server 2022 com função de File Server secundário, fornecendo tolerância a falhas, aumentando o desempenho e redundância para os arquivos da empresa. Para a replicação dos arquivos, pode ser utilizado o serviço DFS (Distributed File System) nativo do Windows Server. A replicação do DFS é um processo que permite que você sincronize arquivos entre vários servidores de arquivos.

14.3. Graylog

Inclusão de um servidor Linux Debian 12 com a solução Graylog, pois é uma ferramenta essencial para auditoria de dados, pois fornece um histórico de todas as atividades que ocorrem em uma rede ou sistema. Os registros de logs podem ser usados para detectar alterações nos dados, verificar a conformidade com regulamentos e investigar incidentes de segurança.

14.4. Antivirus

Inclusão de um antivírus de próxima geração (NGAVs), mantendo assim os endpoints seguros com uma proteção que combina segurança baseada em IA e Machine Learning, permitindo a aprendizagem contínua com as detecções do passado de modo a aperfeiçoar os recursos de prevenção do futuro.

14.5. Backup

Inclusão de uma ferramenta robusta de backup, pois é essencial para proteger os dados das empresas. Ele ajuda a garantir a continuidade dos negócios, reduzir custos e proteger contra perda de dados. Alguns exemplos de ações que podem comprometer os dados são: Falhas de hardware ou software, ataques cibernéticos e até mesmo desastres naturais. A escolha da melhor estratégia de backup depende das necessidades específicas da empresa. Para nosso cenário, escolhemos a ferramenta Veeam Backup & Replication.

14.6. Firewall - HA

Inclusão de um segundo firewall, mantendo alta disponibilidade (HA), deste modo, se um dos firewalls falhar, o outro assumirá automaticamente o controle. Isso garante que a rede permaneça protegida e disponível, mesmo em caso de falha de hardware ou software.

15. PLANO DE AÇÃO

Iniciamos com uma reunião de alinhamento junto a equipe de gerência, abordamos a importância da implementação da política de segurança da rede. Segundo ponto será a ampla divulgação.

Após o alinhamento junto a equipe liderança, a parte de implementação ficará a cargo o setor de TI, o treinamento envolverá o coordenador de TI junto ao DP. Ao término do treinamento, será executado uma avaliação para todos os colaboradores a fim de validar a eficácia do treinamento. Lembrando que o treinamento supracitado tem como objetivo deixar claro todas as diretrizes de segurança de rede, sendo ela física, logica e incluindo boas práticas do dia a dia.

15.1. Cronograma

Todas as tarefas serão definidas em reuniões, e acompanhadas para conferência e realizações efetivas. Uma vez por semana será avaliado a realização das tarefas.

15.2. Semana 1:

Será realizado por etapas, com a duração de 4 semanas, onde todos os analistas estarão comprometidos em concluir as demandas.

Será realizada call semanal para acompanhar a evolução.

15.3. Semana 2: Revisão das configurações de segurança

Revisar as regras de firewall e desabilitar regras com count igual a zero com mais de 45 dias.

Verificar no Active Directory contas com privilégios elevadas, desabilitar e mover para OU Disable contas de usuário e computador que não logam por mais de 45 dias.

Verificar no File Server se os compartilhamentos das pastas estão apenas com grupos de usuários e se possuem irregularidades nas permissões.

Verificar se todos os servidores estão os patches em dia.

15.4. Semana 3: Teste de penetração:

Contratar consultoria externa de red teaming, onde serão realizados ataques diretos contra a infraestrutura de rede e sistemas internos, engenharia social, e-mails de phishing para obter credenciais de login ou instalar malware. A segurança física também será testada, tentando obter acesso físico a empresa e aos terminais usando IDs de funcionários falsos ou clonados ou simplesmente se passando por motorista de entrega, limpador ou construtor.

15.5. Semana 4: Correção

Análise do teste de penetração e correção das falhas identificadas.

Com base no relatório de teste de penetração, verificar como cada item pode ser corrigido, aplicar correções e apresentar relatório com evidências.

CONCLUSÃO

Nesta 5 etapa do projeto de rede segura com foco em segurança da informação no ambiente de rede, o grupo 03, abordou uma estratégia que evidencia, a segurança como o principal ativo da infraestrutura.

Independentemente do tamanho, um projeto de rede deve ser meticulosamente planejado e estruturado para prevenir vulnerabilidades que possam comprometer todo o ambiente de infraestrutura. A implementação de diretrizes de segurança e treinamentos coletivos são passos essenciais frequentemente negligenciados no contexto tecnológico. Nesta fase, concentramos nossa atenção na auditoria das diretrizes já em vigor, incluindo uma revisão abrangente da análise de riscos, planos de contingência e a instituição de uma cultura de segurança de rede que permeie todos os setores da empresa, independentemente de sua área de atuação.

A revisão completa da análise de riscos e a elaboração de planos de contingência são etapas cruciais para assegurar a solidez da rede e minimizar os riscos de vulnerabilidades. Além disso, a instauração de uma cultura de segurança de rede é fundamental para garantir que todos os funcionários estejam cientes dos riscos de segurança e saibam como reagir diante de possíveis incidentes.

No âmbito das medidas de segurança, a utilização de firewall é vital para controlar o tráfego de rede, filtrar conexões indesejadas e proteger contra ameaças externas. O Active Directory desempenha um papel crucial na gestão de identidades, oferecendo controle de acesso e centralizando políticas de segurança. O file server, ao centralizar e gerenciar o armazenamento de dados, requer medidas robustas de segurança para evitar acessos não autorizados. Complementarmente, a presença de um antivírus eficaz é imprescindível para detectar e neutralizar ameaças em tempo real, fortalecendo a defesa contra invasões.

A implementação estratégica dessas ferramentas, aliada a políticas de segurança bem definidas e a um treinamento contínuo dos colaboradores, estabelece uma base sólida para a proteção do ecossistema empresarial contra possíveis ataques cibernéticos.

Como sugestão de continuação desse trabalho, algumas empresas devem ser consultadas para determinar a necessidade de conhecimento atual do profissional de segurança da informação e o que é encontrado hoje no mercado do trabalho. Também avaliar a intenção de investimento financeiro por parte das empresas no profissional contratado para alcançar o nível técnico desejado.

Para o aluno que se forma e tem o desejo de ser um profissional de segurança da informação no mercado do trabalho, recomenda-se o investimento (tempo x dinheiro) em cursos, formações e certificações específicas para a área. Há vários cursos no Brasil de pós-graduação (especialização) em segurança da informação, com duração variando de dez até dezoito meses.

Fora do Brasil, podemos encontrar outros cursos, como o Master of Science in Cyber Security and Information Assurance, da Southern Utah University, com duração de dezesseis meses ao custo total de 45 mil dólares. Outros cursos fora do Brasil têm valores similares.

REFERENCIAS:

Norma ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos;
ASSUNÇÃO, Marcos Flávio Araújo. Guia do Hacker Brasileiro.

Visual Books, 2002. BARBOSA, Pedro. The end of Facebook. Editorial AS, 2013. CABRAL, Carlos; CAPRINO, William. Trilhas em Segurança da Informação: Caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015.

CAMPOS, Andre L. N. Sistema de Segurança da Informação: Controlando os Riscos.

Visual Books, 2006. CERT.BR. Centro de estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha oficial de segurança de redes da Cert.br. Disponível em: <https://cartilha.cert.br/redes/ >

CHIAVENATO, Idalberto. Recursos Humanos: edição compacta. 7. ed. São Paulo: Atlas, 2002. DOMSCHEIT-BERG, Daniel. Nos bastidores da Wikileaks. Leya, 2011.

FACHIN, Odília. Fundamentos de Metodologia. 5.ed. São Paulo: Saraiva, 2006. FONTES, Edison. Políticas e Normas para a Segurança da Informação. Rio de Janeiro: Brasport, 2012.

GEUS, Paulo Lício de; NAKAMURA, Emilio Tissato. Segurança de Redes em ambientes corporativos. São Paulo: Novatec, 2007. GOODRICH, Michael T.; TAMASSIA, Roberto. Introdução à Segurança de Computadores.

JÚNIOR, Elias Daher. A culpa é da Informática: os desafios e caminhos para o gestor de TI. Ebook. Clube de Autores: 2005. Disponível em: <https://books.google.com.br/books?id=DQSvCQAAQBAJeprintsec=frontcover ehl=ptBResource=gbs_ge_summary_recad=0#v=onepageeqef=false>