PUC Minas

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Aluno: André Luiz Dias

Etapa 1

DESENVOLVIMENTO DE UMA POLITICA DE SEGURANÇA EM REDES DE COMPUTADORES

No passado, a maioria das ameaças digitais eram originadas por gênios da computação ou estudantes com muito tempo livre.

Confirme o tempo foi passando, o conhecimento foi sendo disseminado e. hoje, estas ameaças se multiplicaram e podem ser iniciadas por praticamente qualquer pessoa que tenha acesso a Internet. Não é novidade, portanto, que o assunto de segurança de redes venha ganhando destaque nos últimos anos. Empresas buscam especialistas em segurança para ajuda-las a conter o crescente número de ameaças.

A maior preocupação hoje é a clara alteração na motivação dos criminosos virtuais, antes motivados pelo desafio, estes agiam normalmente sozinhos. Hoje, a motivação é o ganho financeiro alcançado por meio de acesso a informações sigilosas, desvio eletrônico de recursos, roubo de identidade, chantagem por meio de ataques coordenados à servidores vitais, dentre muitos outros.

Podemos resumir a importância de uma política de segurança em redes de computadores com os seguintes tópicos:

1- Controle físico de acesso;
2- Rede elétrica estabilizada e com redundância;
3- Rede segmentada;
4- Proteção contra ameaças cibernéticas;
5- Plano de resposta a incidentes;
6- plano de resposta a incidentes;
7- Políticas de Senhas;

1 INTRODUÇÃO

A política de segurança é um conjunto de diretrizes, regras e práticas estabelecidas para proteger sistemas, dados e informações em um ambiente digital. Ela desempenha um papel crucial na preservação da integridade, confidencialidade e disponibilidade das informações, especialmente em um cenário onde ameaças cibernéticas são cada vez mais complexas e disseminadas. Ao definir estratégias de prevenção, detecção e resposta a incidentes de segurança, a política de segurança cria um alicerce para a construção de um ambiente tecnológico confiável, garantindo a continuidade dos negócios, a conformidade com regulamentações e a confiança dos usuários.

2 CONTROLE DE ACESSO FÍSICO

O controle de acesso físico desempenha um papel fundamental na segurança.

2.1 Segurança Aprimorada: Os sistemas de controle de acesso baseados em digitais e cartões oferecem um nível mais alto de segurança em comparação com métodos tradicionais, como chaves físicas. Isso ocorre porque é mais difícil replicar ou falsificar impressões digitais ou cartões de acesso.

2.2 Identificação Individual: Impressões digitais e cartões são formas únicas de identificação biométrica e eletrônica, respectivamente. Isso permite a autenticação individual precisa, eliminando a possibilidade de compartilhamento de senhas ou chaves.

2.3 Registro de Auditoria: Os sistemas de controle de acesso digital normalmente mantêm registros detalhados das atividades de entrada e saída. Isso possibilita a criação de uma trilha de auditoria que rastreia quem entrou ou saiu de determinada área, o que pode ser valioso para investigações de incidentes.

2.4 Flexibilidade e Gerenciamento: Os administradores podem gerenciar de maneira mais eficiente as permissões de acesso. Por exemplo, se um cartão for perdido ou um funcionário deixar a empresa, é mais fácil revogar o acesso imediatamente, impedindo o acesso não autorizado.

2.5 Conveniência: O uso de digitais ou cartões é mais conveniente para os usuários do que a necessidade de carregar várias chaves ou lembrar senhas complexas. Isso aumenta a eficiência e a facilidade de uso.

2.6 Integração com Outros Sistemas: Muitos sistemas de controle de acesso podem ser integrados a outras soluções de segurança, como

sistemas de vigilância por vídeo ou alarmes, criando um ecossistema de segurança mais abrangente.

2.7 Redução de Riscos de Perda ou Roubo: A utilização de impressões digitais ou cartões dificulta ações de intrusos ou pessoas não autorizadas que tentam acessar áreas restritas, reduzindo significativamente os riscos de perda, roubo ou vandalismo.

2.8 Prevenção de Invasões Internas: O controle de acesso físico ajuda a prevenir invasões internas, impedindo que funcionários mal-intencionados ou ex-funcionários acessem áreas sensíveis.

O cadastro será divido por digitais e cartões, onde, os colaboradores serão cadastrados com através de biometria apenas após a sua contratação, já os visitantes terão seu acesso via cartão físico cadastrado na recepção e de forma temporária.

3 REDE ELÉTRICA ESTABILIZADA E COM REDUNDÂNCIA

Uma rede elétrica com redundância desempenha um papel crítico na operação contínua e na proteção dos equipamentos e sistemas de uma empresa. A redundância na rede elétrica envolve ter fontes de energia alternativas ou backups para garantir que, mesmo em caso de falha na fonte principal de energia, as operações não sejam interrompidas. A importância dessa redundância pode ser destacada da seguinte forma:

3.1 Proteção de Equipamentos Sensíveis: Muitos equipamentos eletrônicos são sensíveis a flutuações de energia, quedas e surtos. Uma rede elétrica com redundância reduz o risco de danos a equipamentos caros e importantes, prolongando sua vida útil e evitando a necessidade de substituições frequentes.

3.2 Manutenção Planejada: A redundância permite que a manutenção e reparos na rede elétrica principal sejam realizados sem interromper as operações. Isso é possível ao alternar temporariamente para a fonte de energia de backup durante as atividades de manutenção, minimizando o impacto nas operações diárias.

3.3 Proteção de Dados: Além da proteção física temos a proteção de dados, evitando assim o desligamento incorreto ou mesmo a queima de servidores ou ativos de redes.

O sistema deve contar com um nobreak e um gerador movido a diesel, a função do nobreak é estabilizar e manter a energia (rampa) até que o gerador entre em funcionamento em uma falta de energia, por sua vez o gerador de uso em standby monitora a rede externa, acionando automaticamente em caso de quedas da rede.

4 SEGMENTAÇÃO DE REDE

A segmentação de rede oferece vantagens significativas em termos de segurança, conformidade, controle e desempenho, tornando-a uma prática valiosa para proteger ativos e dados valiosos em um ambiente digital cada vez mais complexo.

4.1 Segurança Aprimorada: A segmentação de rede ajuda a reduzir a superfície de ataque, limitando o movimento lateral de ameaças. Caso um segmento seja comprometido, as outras partes da rede permanecem protegidas, isolando o impacto de possíveis ataques.

4.2 Isolamento de Ativos Críticos: Ativos de alto valor ou sensíveis podem ser isolados em segmentos separados, garantindo que apenas os usuários autorizados tenham acesso. Isso protege informações confidenciais de ameaças internas e externas.

4.3 Controle de Acesso Granular: A segmentação permite a implementação de políticas de controle de acesso mais granulares. Isso significa que apenas os usuários e dispositivos com permissão podem acessar determinados segmentos, reduzindo a exposição a ataques.

4.4 Prevenção e Mitigação de Ataques: A segmentação limita a propagação de malware e ataques cibernéticos. Se um dispositivo em um segmento for infectado, a disseminação para outros segmentos é impedida, facilitando a contenção e a resposta a incidentes.

4.5 Maior Visibilidade: Segmentar a rede permite um monitoramento mais eficaz de tráfego e atividades em cada segmento. Isso ajuda a identificar comportamentos anômalos e potenciais ameaças mais rapidamente.

4.6 Melhoria no Desempenho: Segmentar a rede pode resultar em melhor desempenho, pois o tráfego é isolado e não sobrecarrega toda a rede. Isso

é especialmente útil para tráfego intensivo, como streaming de vídeo ou transferências de dados pesadas.

Com a utilização de Vlans temos uma maior segurança, não misturando o tráfego de redes, custo reduzido pois um único equipamento pode separar logicamente vários segmentos da rede, melhor desempenho já que os domínios de broadcast serão aplicados por vlans.

5 PROTEÇÃO CONTRA AMEAÇAS CIBERNÉTICAS

A proteção contra ameaças cibernéticas é uma prioridade fundamental em qualquer ambiente digital atual. Com o aumento constante da sofisticação das ameaças, é essencial implementar estratégias abrangentes para mitigar riscos e proteger sistemas, dados e informações.

5.1 Firewall: Implementar firewalls de rede é um primeiro passo crucial. Isso permite que você controle o tráfego que entra e sai da rede, bloqueando atividades suspeitas.

5.2 Antivírus Atualizado: Manter soluções antivírus atualizadas é vital. Essa ferramenta identifica e remove ameaças conhecidas, bem como detectam comportamentos anômalos que podem indicar atividades maliciosas.

5.3 Atualizações e Patches Regulares: Manter sistemas operacionais e software atualizados com os últimos patches de segurança é uma defesa essencial. Muitos ataques exploram vulnerabilidades conhecidas que poderiam ter sido evitadas com atualizações apropriadas.

Implementação de firewall físico, com regras configuradas pré configuradas analisando a camada de nível 3, antivírus sempre com suas últimas atualizações e varredura heurística habilitada, atualizações de S.O e programas, lembrando sempre de usar software licenciados e originais.

6 PLANO DE RESPOSTA A INCIDENTES

Um plano de resposta a incidentes é um conjunto organizado de procedimentos e diretrizes que uma organização segue para identificar, conter, mitigar e se recuperar de incidentes de segurança cibernética. Ele é projetado para minimizar os impactos de incidentes de segurança e garantir que a organização esteja preparada para lidar com ameaças em rápida evolução.

6.1 Equipe de Resposta a Incidentes: Designe uma equipe responsável pela execução do plano de resposta a incidentes.

6.2 Classificação de Incidentes: Crie uma estrutura de classificação para avaliar a gravidade e o impacto potencial de diferentes tipos de incidentes. Isso ajuda a priorizar as respostas de acordo com a urgência.

6.3 Procedimentos de Notificação: Defina um processo claro para notificar a equipe de resposta a incidentes quando um incidente for detectado. Isso pode envolver sistemas de alerta, canais de comunicação e responsabilidades claras para quem deve ser informado.

6.4 Identificação e Avaliação: Estabeleça procedimentos para identificar e avaliar a natureza do incidente. Isso envolve a coleta de evidências, análise forense e determinação do escopo do incidente.

6.5 Isolamento e Contenção: Tome medidas para isolar o incidente e evitar que ele se espalhe para outras partes da rede. Isso pode envolver a desconexão de sistemas comprometidos ou a criação de segmentos de rede isolados.

6.6 Mitigação e Eliminação: Desenvolva estratégias para mitigar os efeitos do incidente e eliminar a ameaça. Isso pode envolver a aplicação de correções, atualizações ou patches para sistemas afetados.

O serviço de pronta resposta traz agilidade na ocorrência de qualquer evento que exija a presença de um agente especializado que vai se deslocar imediatamente para o local, se possível ter duas equipes.

7 POLITICAS DE SENHAS

Grande parte das violações na rede e nos sistemas empresariais ocorre devido a comportamento humano inadequado, incluindo senhas consideradas fracas. Senhas fáceis, que possuem dados como datas de nascimento, endereços ou outras informações pessoais dos usuários podem ser facilmente descobertas por criminosos.

7.1 ter no mínimo 8 caracteres: Senhas menores são muito fáceis de serem lembradas, porém fáceis de ser hackeadas.

7.2 ter pelo menos 1 letra maiúscula e uma minúscula: para dificultar a quebra de senha é recomendado o uso de uma ou mais letras maiúsculas ou minúsculas.

7.3 usar números e símbolos: quanto mais complexa a senha melhor será sua segurança.

Todas as senhas terão um prazo de 90 dias corridos, passados esse período o usuário que não trocar sua senha, não terá mais acesso ao sistema. Deve-se criar um método próprio para elaborar e lembrar sua senha, de modo que o usuário não precise anotar em nenhum local.

8 TREINAMENTOS CONSTANTE

A maioria das empresas dedica grande quantidade de tempo e finanças na implementação de software para proteger suas informações de segurança, com orçamentos médios de TI para segurança em torno de 10%. No entanto, 'hardware humano' é de longe o elemento mais vulnerável de qualquer negócio e as empresas devem operar com base na prevenção ao invés da cura.
O erro humano é a causa de até 95% das violações de segurança cibernética e, com simples cursos de treinamento de conscientização, esse número pode ser reduzido drasticamente.

8 REFERENCIAS

BOYLES, Tim. et al. Cisco CCNP Certification Library. [s.1]): Cisco Press

CERF, Vinton How the Internet Came to Be.

LAMMLE Todd. Cisco CCNA Study Guide. [s.1.]: Sybex,

MINOLI Daniel; SCHMIDT, Andrew. Internet Architectures.

[S. 1]:Exam Certification Guide. Cisco

FILIPPETTI. M. A. CCNA 4.1 GUIA COMPLETO DE ESTUDO

Visual Books

ODOM Wend. CCENT/CCNA ICND1

Alta Books