PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Aluno: André Luiz Dias

Etapa 3

Melhorias nas politicas de segurança

Após a implementação de algumas politicas de segurança e testes vamos descrever o que mais será implementado para uma melhora na segurança.

Sumário

1 INTRODUÇÃO

Nesta etapa vamos acrescentar mais segurança na rede, conforme os tópicos abaixo :

- Firewalls de Rede;
- Sistema de Detecção de Intrusões (IDS) e Sistema de Prevenção de Intrusões (IPS);
- Autenticação de Multi-Fatores (MFA);
- Gestão de Identidade e Acesso (IAM);
- Antivírus;
- Backup e Recuperação de Dados;
- Monitoramento e Registro de Atividades;
- Atualizações e Patch Management;

2 - FIREWALLS DE REDE

Os firewalls de rede são dispositivos essenciais no contexto da segurança da informação. Eles atuam como barreiras entre redes, controlando o tráfego de dados com base em regras predefinidas. Essas regras determinam quais comunicações são permitidas ou bloqueadas, visando proteger uma rede contra tráfego não autorizado e potenciais ameaças.

2.1 Principais Características:

Filtragem de Pacotes:

Os firewalls analisam pacotes de dados que entram ou saem da rede. Cada pacote é verificado de acordo com as regras de segurança estabelecidas.

Estabelecimento de Políticas:

As regras e políticas do firewall são configuradas para determinar quais tipos de tráfego são permitidos ou bloqueados. Isso pode incluir restrições com base em portas, protocolos e endereços IP.

Prevenção de Acesso Não Autorizado:

Impedem a entrada de tráfego não autorizado, bloqueando conexões que não atendem aos critérios especificados nas políticas do firewall.

Segurança em Nível de Aplicação:

Alguns firewalls modernos oferecem recursos avançados de inspeção em nível de aplicação, permitindo uma análise mais profunda do tráfego para identificar ameaças específicas.

NAT (Network Address Translation):

O NAT é frequentemente usado em firewalls para mascarar os endereços IP internos, protegendo a identidade da rede interna para usuários externos.

VPN (Virtual Private Network):

Alguns firewalls incluem funcionalidades VPN, permitindo a criação de túneis seguros para comunicações criptografadas entre redes.

2.2 Benefícios:

Segurança:

Protege a rede contra ameaças externas, como ataques de hackers e malware.

Controle de Tráfego:

Permite um controle granular sobre o tráfego de dados, garantindo que apenas comunicações autorizadas ocorram.

Privacidade:

Ajuda a preservar a privacidade da rede interna, limitando o que é visível para usuários externos.

Conformidade:

Auxilia na conformidade com regulamentações de segurança, garantindo que padrões e políticas sejam seguidos.

Em resumo, os firewalls de rede desempenham um papel fundamental na proteção contra ameaças cibernéticas, garantindo a segurança e integridade das redes corporativas.

3-SISTEMA DE DETECÇÃO DE INTRUSÕES (IDS) E SISTEMA DE PREVENÇÃO DE INTRUSÕES (IPS)

Os Sistemas de Detecção de Intrusões (IDS) e os Sistemas de Prevenção de Intrusões (IPS) são componentes essenciais em arquiteturas de segurança da informação, projetados para identificar e responder a atividades suspeitas em uma rede. Ambos desempenham papéis cruciais na proteção contra ameaças cibernéticas, mas suas funções principais diferem.

3.1 Sistema de Detecção de Intrusões (IDS):

Descrição:

O IDS é um dispositivo ou aplicativo que monitora o tráfego de rede em busca de padrões de atividade suspeitos ou anômalos. Ele atua como um "detector de alarme" e alerta os administradores sobre possíveis intrusões ou violações de segurança.

Funcionamento:

O IDS analisa pacotes de dados e eventos na rede, comparando-os com padrões predefinidos ou comportamentos normais. Quando detecta atividades fora do padrão, gera alertas ou notificações para que a equipe de segurança possa tomar medidas corretivas.

Principais Características:

Monitoramento passivo: Observa e analisa o tráfego sem interferir no fluxo de dados.

Geração de alertas: Notifica administradores sobre atividades suspeitas.

Análise de padrões: Compara comportamentos com perfis conhecidos para identificar desvios.

3.2 Sistema de Prevenção de Intrusões (IPS):

Descrição:

O IPS é uma evolução do IDS e vai além da detecção, pois tem a capacidade de bloquear ou prevenir automaticamente atividades identificadas como intrusivas. Ele age como uma "barreira ativa" contra ameaças, bloqueando ou modificando o tráfego malicioso.

Funcionamento:

O IPS utiliza as informações do IDS para tomar ações proativas. Pode rejeitar pacotes específicos, encerrar conexões ou até mesmo ajustar as configurações do firewall para bloquear automaticamente determinados tipos de tráfego.

3.3 Principais Características:

Ação proativa: Além da detecção, pode agir automaticamente para bloquear ou prevenir ameaças.

Bloqueio de tráfego: Pode tomar medidas para interromper a execução de atividades maliciosas.

Resposta em tempo real: Age instantaneamente para proteger a rede contra ameaças identificadas.

3.4 Diferenças Principais:

O IDS é principalmente um observador passivo que alerta sobre atividades suspeitas.

O IPS vai além da detecção, agindo proativamente para bloquear ou prevenir automaticamente atividades maliciosas.

Ambos desempenham papéis complementares na proteção de uma rede, garantindo uma abordagem abrangente para a segurança cibernética.

4 - AUTENTICAÇÃO DE MULTI-FATORES (MFA):

A Autenticação de Multi-Fatores (MFA) é uma abordagem de segurança que exige que os usuários forneçam múltiplos métodos de verificação de identidade durante o processo de autenticação. Em vez de depender apenas de uma senha, a MFA adiciona camadas adicionais de segurança, aumentando a robustez do processo de verificação. Essa abordagem visa reduzir significativamente o risco de acesso não autorizado, mesmo que um fator de autenticação seja comprometido.

4.1 Principais Componentes da MFA:

Fator de Conhecimento (Algo que o usuário sabe):

Senha: A senha tradicional é um exemplo de fator de conhecimento. O usuário deve inserir uma combinação secreta de caracteres para provar que conhece a informação confidencial associada à conta.

Fator de Posse (Algo que o usuário possui):

Token de Segurança: Um dispositivo físico ou aplicativo gerador de códigos que gera um código único que muda regularmente. O usuário precisa possuir esse dispositivo ou aplicativo para realizar a autenticação.

Fator de Inerência (Algo que o usuário é):

Biometria: Características físicas únicas do usuário, como impressões digitais, reconhecimento facial, íris, voz, ou outras características biométricas. Esses fatores dependem das características físicas ou comportamentais do usuário.

4.2 Benefícios da MFA:

Maior Segurança:

Adiciona camadas de segurança, tornando mais difícil para os invasores obterem acesso não autorizado, mesmo que uma senha seja comprometida.

Redução de Riscos:

Minimiza o impacto de violações de credenciais, pois os invasores precisariam superar múltiplos fatores de autenticação.

Conformidade:

Atende a requisitos regulatórios e padrões de segurança, que muitas vezes exigem métodos adicionais de verificação de identidade.

Proteção Contra-Ataques de Engenharia Social:

Dificulta a eficácia de ataques baseados em engenharia social, onde os invasores tentam obter informações de login dos usuários.

5 - GESTÃO DE IDENTIDADE E ACESSO (IAM):

A Gestão de Identidade e Acesso (IAM) é um conjunto de processos, políticas e tecnologias que visa gerenciar e garantir a identificação e permissões de acesso de usuários em um ambiente de tecnologia da informação. O objetivo principal da IAM é garantir que as pessoas certas tenham o acesso apropriado aos recursos certos, enquanto, ao mesmo tempo, protege os dados e sistemas contra acessos não autorizados.

5.1 Principais Componentes da IAM:

Provisionamento de Identidade:

Automatização do processo de atribuição e gerenciamento de identidades de usuários, incluindo a criação, modificação e desativação de contas.

Autenticação:

Verificação da identidade de um usuário antes de conceder o acesso. Isso pode envolver senhas, autenticação de dois fatores (2FA), autenticação biométrica, entre outros métodos.

Autorização:

Determinação das permissões e acessos específicos que um usuário autenticado tem dentro do sistema ou rede. Isso envolve a definição de papéis, privilégios e políticas de acesso.

Administração de Contas e Senhas:

Gerenciamento centralizado de contas de usuários, incluindo a redefinição de senhas, a recuperação de contas e a aplicação de políticas de segurança.

Auditoria e Monitoramento:

Acompanhamento e registro das atividades de usuários para garantir a conformidade com políticas de segurança, além de detectar e responder a atividades suspeitas.

Gerenciamento de Ciclo de Vida da Identidade:

Controle de todas as fases da existência de uma identidade, desde a criação até a desativação, garantindo a consistência e segurança ao longo do tempo.

5.2 Benefícios da IAM:

Segurança Aprimorada:

Reduz o risco de acesso não autorizado e violações de segurança, garantindo que apenas usuários autorizados tenham acesso aos recursos.

Eficiência Operacional:

Automatiza processos de provisionamento e desativação, economizando tempo e recursos operacionais.

Conformidade:

Ajuda as organizações a cumprir regulamentações e padrões de segurança ao garantir que as políticas e controles sejam aplicados.

Melhoria da Experiência do Usuário:

Facilita o acesso seguro, oferecendo uma experiência de usuário mais eficiente e sem complicações.

A IAM desempenha um papel crucial em ambientes corporativos, especialmente em organizações com um grande número de usuários e sistemas, garantindo a segurança, eficiência e conformidade.

6 - ANTIVÍRUS:

Os antivírus são programas de software projetados para detectar, prevenir e remover software malicioso (malware) de computadores e sistemas. O termo "vírus" historicamente se referia a um tipo específico de malware, mas, ao longo do tempo, o termo "antivírus" evoluiu para abranger uma variedade de ameaças, incluindo vírus, worms, cavalos de Troia, spyware, adware e outros tipos de software indesejado.

6.1 Principais Funcionalidades dos Antivírus:

Varredura de Arquivos e Programas:

Os antivírus examinam arquivos e programas em busca de padrões de código malicioso ou comportamentos suspeitos.

Atualizações de Definições de Vírus:

Mantêm uma base de dados atualizada de definições de vírus para reconhecer novas ameaças à medida que surgem.

Quarentena e Remoção:

Isolam arquivos infectados em quarentena para evitar a propagação e, quando possível, removem ou neutralizam as ameaças.

Proteção em Tempo Real:

Monitoram a atividade em tempo real para identificar e bloquear ameaças à medida que tentam infectar o sistema.

Firewall Pessoal:

Alguns antivírus incluem firewalls pessoais para adicionar uma camada extra de proteção contra ameaças online.

7-Backup e Recuperação de Dados

Frequência:

Determina com que frequência os backups são realizados. Pode variar de backups contínuos (em tempo real) a backups programados diariamente, semanais ou conforme necessário.

7.1 Métodos de Backup:

Backup Completo: Copia todos os dados selecionados.

Backup Incremental: Cópias apenas dos dados modificados desde o último backup.

Backup Diferencial: Cópias dos dados modificados desde o último backup completo.

Local de Armazenamento:

Pode incluir discos rígidos externos, servidores locais, nuvem ou serviços de armazenamento dedicados.

Segurança do Backup:

Os backups devem ser protegidos contra acesso não autorizado para garantir a segurança dos dados de backup.

Recuperação de Dados:

A recuperação de dados envolve a restauração dos dados a partir dos backups em caso de perda, seja devido a falhas de hardware, erro humano, ataques de malware ou outros incidentes.

7.2 Principais Elementos da Recuperação de Dados:

Tempo de Recuperação:

Refere-se à rapidez com que os dados podem ser restaurados. O tempo de recuperação é crucial para minimizar o impacto de interrupções nos negócios.

Pontos de Recuperação:

Indica os momentos específicos nos quais os dados foram copiados. Ter vários pontos de recuperação permite restaurar os dados para diferentes estados.

Procedimentos de Recuperação:

Documentação detalhada que descreve os passos necessários para iniciar e concluir com êxito o processo de recuperação.

Testes de Recuperação:

A realização regular de testes para garantir que os procedimentos de recuperação sejam eficazes e que os dados podem ser restaurados com sucesso.

7.3 Importância do Backup e Recuperação de Dados:

Prevenção de Perda de Dados:

Protege contra a perda irreversível de dados devido a falhas de hardware, exclusões acidentais, ataques de malware, entre outros.

Continuidade dos Negócios:

Minimiza o tempo de inatividade, permitindo a rápida restauração dos dados essenciais em caso de interrupções.

Segurança e Conformidade:

Ajuda a cumprir requisitos regulatórios e a manter a integridade e confidencialidade dos dados.

Proteção contra Ransomware:

Oferece uma camada adicional de defesa contra ataques de ransomware, permitindo a restauração de dados sem ceder a exigências de resgate.

Recuperação de Desastres:

Desempenha um papel vital na recuperação de dados após eventos catastróficos, como incêndios, inundações ou outras situações de desastre.

A implementação eficaz de estratégias de backup e recuperação é fundamental para a segurança e resiliência dos dados em ambientes pessoais e empresariais.

8-Monitoramento e Registro de Atividades

O monitoramento de atividades refere-se à observação em tempo real das operações e interações em sistemas de tecnologia da informação. Este processo permite que as organizações identifiquem comportamentos normais e anômalos, detectem possíveis ameaças e monitorem o desempenho dos sistemas.

8.1 Principais Elementos do Monitoramento de Atividades:

Tráfego de Rede:

Monitoramento do tráfego de dados na rede para identificar padrões de comunicação, tráfego incomum e possíveis ameaças.

Registros de Logs:

Acompanhamento de logs de sistemas, aplicativos e dispositivos para registrar eventos releva ntes, como tentativas de login, alterações de configuração e atividades do usuário.

Monitoramento de Servidores:

Observação contínua do desempenho e integridade dos servidores para detectar possíveis problemas, ataques ou comportamentos suspeitos.

Segurança Física:

Monitoramento de câmeras de segurança, sistemas de controle de acesso e outros dispositivos para garantir a segurança física de instalações.

Detecção de Anomalias:

Utilização de ferramentas e algoritmos para identificar padrões de comportamento que se desviam do normal, indicando possíveis atividades maliciosas.

Registro de Atividades:

O registro de atividades, também conhecido como logging, envolve a criação e armazenamento de registros detalhados de eventos e ações em sistemas e redes. Esses registros são valiosos para a análise forense, investigação de incidentes e auditorias de segurança.

8.2 Principais Elementos do Registro de Atividades:

Logs de Eventos:

Criação de logs que registram eventos específicos, como autenticações, tentativas de acesso não autorizado, alterações de configuração e atividades críticas.

Timestamps:

Inclusão de informações de data e hora precisas nos registros para facilitar a análise cronológica de eventos.

Detalhes do Usuário:

Registro de informações relacionadas a usuários, como identificadores, endereços IP, nomes de usuário e outras informações de identificação.

Origem e Destino:

Registro dos pontos de origem e destino de atividades, como endereços IP, para rastrear a comunicação entre sistemas.

Nível de Severidade:

Atribuição de níveis de severidade aos eventos registrados para priorizar a resposta e investigação de acordo com a gravidade.

8.*3 Importância do Monitoramento e Registro de Atividades:*

Detecção Prévia de Ameaças:

Permite a identificação precoce de atividades maliciosas, possibilitando respostas rápidas antes que causem danos significativos.

Investigação Forense:

Facilita a análise forense, fornecendo registros detalhados para reconstruir eventos, determinar a causa raiz de incidentes e apoiar investigações.

Conformidade e Auditoria:

Atende aos requisitos regulatórios e auxilia em auditorias internas e externas, fornecendo uma trilha de auditoria detalhada.

Melhoria Contínua:

Oferece insights sobre o desempenho e a eficácia das medidas de segurança, permitindo ajustes e melhorias contínuas.

Resposta a Incidentes:

Facilita uma resposta eficaz a incidentes de segurança, fornecendo informações detalhadas sobre o que ocorreu e como remediar.

Ao implementar uma estratégia eficaz de monitoramento e registro de atividades, as organizações fortalecem sua postura de segurança, melhoram a resiliência contra ameaças e promovem a transparência nas operações de TI.

9-Atualizações e Patch Management;

Atualizações:

As atualizações referem-se a modificações ou melhorias aplicadas a software, sistemas operacionais, aplicativos ou firmware para corrigir problemas, adicionar recursos, aprimorar o desempenho e, o mais importante, corrigir vulnerabilidades de segurança. As atualizações são lançadas periodicamente pelos desenvolvedores de software para garantir que os sistemas estejam protegidos contra ameaças conhecidas e funcionem de maneira eficiente.

9.1 *Principais Elementos das Atualizações:*

Correções de Segurança:

Incluem patches para corrigir vulnerabilidades de segurança que poderiam ser exploradas por ameaças cibernéticas.

Melhorias de Desempenho:

Podem otimizar o desempenho do software, corrigir bugs e proporcionar uma experiência mais suave aos usuários.

Novos Recursos:

Introduzem novas funcionalidades e recursos para melhorar a usabilidade e a eficácia do software.

Compatibilidade:

Atualizações são muitas vezes lançadas para garantir a compatibilidade com hardware mais recente, sistemas operacionais e padrões tecnológicos.

Atualizações de Banco de Dados:

Em sistemas que usam bancos de dados, as atualizações podem incluir melhorias de desempenho, otimizações e correções de segurança.

9.2 *Patch Management:*

O Patch Management refere-se ao processo de gerenciamento e aplicação de patches (correções de software) em um ambiente de TI. Este processo é crucial para manter a segurança, estabilidade e integridade dos sistemas, garantindo que as vulnerabilidades conhecidas sejam corrigidas de forma oportuna.

9.3 *Principais Elementos do Patch Management:*

Identificação de Vulnerabilidades:

Monitoramento constante para identificar vulnerabilidades em software instalado e sistemas.

Priorização de Patches:

Avaliação da gravidade e impacto das vulnerabilidades para priorizar a aplicação de patches críticos.

Testes Prévios:

Realização de testes em ambientes controlados para garantir que a aplicação de patches não cause problemas inesperados nos sistemas.

Implementação Gradual:

Aplicação gradual de patches em ambientes de produção, começando por sistemas menos críticos, para minimizar riscos.

Registro e Auditoria:

Manutenção de registros detalhados de todas as atividades relacionadas a patches para fins de auditoria e conformidade.

Automação:

Uso de ferramentas de automação para simplificar o processo de aplicação de patches e garantir conformidade com políticas de segurança.

Monitoramento Contínuo:

Monitoramento constante para garantir que os sistemas permaneçam atualizados e seguros após a aplicação de patches.

9.4 *Importância de Atualizações e Patch Management:*

Mitigação de Vulnerabilidades:

Corrige vulnerabilidades conhecidas que podem ser exploradas por ameaças cibernéticas.

Resposta a Ameaças Emergentes:

Permite resposta rápida a novas ameaças, pois as atualizações muitas vezes incluem correções para exploits recentemente descobertos.

Estabilidade do Sistema:

Mantém a estabilidade e o desempenho dos sistemas ao corrigir bugs e problemas conhecidos.

Conformidade com Regulamentações:

Ajuda a cumprir requisitos regulatórios que exigem a aplicação de patches de segurança.

Prevenção de Ataques:

Reduz a superfície de ataque, tornando mais difícil para os invasores explorarem vulnerabilidades conhecidas.

Eficiência Operacional:

Melhora a eficiência operacional, automatizando o processo de aplicação de patches e minimizando interrupções nos negócios.

Ao implementar uma estratégia robusta de atualizações e patch management, as organizações fortalecem significativamente a segurança de seus sistemas, reduzem a exposição a ameaças cibernéticas e garantem um ambiente operacional mais confiável e resiliente.

10 REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 17799:2000: **Tecnologia da Informação – Código de Prática para Gestão da segurança de Informação**. Rio de Janeiro, 2001.

ABNT NBR ISO/IEC 27005: **Tecnologia da Informação- Técnicas de Segurança-Gestão de Risco de Segurança da Informação**. Rio de Janeiro, 2008.

BAUER, C. A. Política de segurança da informação para redes corporativas.
Trabalho de conclusão de curso – Centro Universitário Feevale, 2006.

BRASIL. Tribunal de Contas da União. **Boas Práticas de Segurança da Informação/ Tribunal de Contas da União**. 4. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2012.

BORGES, A. **Ataque de fixação de sessão**. Revista Linux. 2014. Disponível em: < http://www.linux-magazine.com.br/images/uploads/pdf_aberto/LM_92_14_15_02_col-alexborges.pdf >. Acessado em: 2 Jun. 2014.

BROWN, T; GALITZ, G. **O farejador de vulnerabilidades OpenVAS**. Linux Magazine, São Paulo, Abr. 2010.

CABRAL, L.; NÓBREGA, A.; SOARES, R. **Efetuando uma Implementação Segura do Protocolo SNMP em Roteadores Cisco: Da teoria à prática**. Unibratec, Recife, 2012.

CARISSIMI, A. S.; ROCHOL, J.; GRANVILLE, L. Z. **Redes de computadores: Volume 20 da Série Livros didáticos informática UFRGS.** Porto Alegre: Bookman, 2009.

CERT.org (2002). **Software Engineering Institute.CERT/CC advisories: Vulnerabilities in Various Implementations of the RADIUS Protocol**. Disponível em: < http://www.cert.org/historical/advisories/CA-2002-06.cfm >. Acessado em: 13 Jun. 2014.

CHESWICK, W. R.; BELLOVIN, S. M.; RUBIN, A. D. **Firewalls e Segurança na Internet: Repelindo o Hacker ardiloso**. 2 ed. Porto Alegre: Editora Bookman Companhia, 2005.