Política de Segurança de Rede

Conteúdo

1 Introdução

O uso de redes é uma parte essencial dos negócios do dia a dia da Cobmais. As redes não apenas conectam, internamente, muitos dos componentes e processos de negócios, mas também vincula a organização a seus fornecedores, clientes, partes interessadas e ao mundo externo.

As redes da organização evoluíram ao longo de um período de tempo para se tornar um sistema circulatório da empresa, transportando as informações para onde precisam ir e permitindo que os negócios sejam realizados de forma eficaz.

Mas o fato de tantas informações percorrerem nossas redes, as torna um alvo para aqueles que tentam roubar essas informações e atrapalhar nossos negócios. Portanto, essas redes precisam ser protegidas para garantir que a confidencialidade, integridade e disponibilidade das nossas informações sejam garantidas a todo momento.

A proteção efetiva de nossas redes exige que adotemos boas práticas de segurança da informação e garantimos que todos os envolvidos sigam essas práticas.

Essa política define as regras e os padrões da Cobmais para proteção da rede e atua como um guia para aqueles que criam e mantêm nossa infraestrutura de TI. Seu público-alvo é o pessoal de gerenciamento e suporte de TI e segurança da informação que implementará e manterá as defesas da organização.

Como um provedor de serviços de nuvem (PSN), essa política também se aplica aos métodos usados para projetar e criar as redes físicas e virtuais.

Esse controle se aplica a todos as operações, pessoas e processos que constituem os sistemas de informações da organização, incluindo membros do conselho, diretores, funcionários, fornecedores e outros terceiros que têm acesso aos sistemas da Cobmais

As políticas e procedimentos a seguir são relevantes para este documento:

- *Política de dispositivos móveis*
- *Política anti-malware*

2 Política de Segurança de Rede

2.1 Projeto de Segurança de Rede

O design de redes é um processo complicado que requer um bom conhecimento dos princípios e tecnologia de rede. Cada projeto provavelmente será diferente, com base em um conjunto específico de requisitos estabelecidos no início do processo. Esta política não tenta especificar como redes individuais devem ser projetadas e construídas, mas fornece orientação para padrões que devem ser usados.

2.1.1 Requisitos

Um projeto de rede deve se basear em uma definição clara de requisitos, incluindo os seguintes fatores relacionados à segurança:

- A classificação da informação a ser transportada através da rede e acessada através dela
- Uma avaliação de risco das ameaças potenciais à rede, levando em consideração quaisquer vulnerabilidades inerentes
- O nível de confiança entre os diferentes componentes ou organizações que serão conectadas
- A expansão geográfica da rede
- Os controles de segurança nos locais onde a rede será acessada
- Recursos de segurança de computadores ou dispositivos existentes que serão usados para acesso

Os requisitos devem ser documentados e acordados antes do início do trabalho de design.

2.1.2 Defesa em Profundidade

Uma abordagem de "Defesa em Profundidade" será adotada para segurança de rede, através da qual várias camadas de controles são usadas para garantir que a falha de um único componente não comprometa a rede. Por exemplo, os firewalls de rede podem ser complementados por firewalls de software baseados em servidores hospedados, a fim de fornecer vários níveis de proteção.

Em pontos chave da rede, uma abordagem de "diversidade de defesa" também deve ser adotada para que as vulnerabilidades sejam minimizadas. Por exemplo, isso pode envolver o uso de firewalls de diferentes fornecedores, de modo que, se uma vulnerabilidade for explorada em um

dispositivo, o outro não estará sujeito a ela. Isso pode ser estendido para o uso de mais de um scanner de vírus de rede.

2.1.3 Segregação em rede

Uma rede consistirá de um conjunto de redes menores segregadas umas das outras com base em níveis de confiança ou limites organizacionais (ou ambos).

Para uma rede grande, isso pode ser alcançado usando domínios separados, particularmente onde as redes de organizações separadas estão sendo vinculadas. Um nível apropriado de confiança deve ser configurado no nível do domínio e os perímetros de domínio devem ser protegidos usando um firewall, quando apropriado.

Nas redes, as redes locais virtuais (RLV) serão usadas para segregar as unidades organizacionais.

Em um ambiente de nuvem, é importante que os requisitos para segregar redes para obter isolamento de inquilino sejam definidos e a capacidade do provedor de serviços de nuvem de atender a esses requisitos seja verificada.

Onde a Cobmais está agindo como um PSN, é importante impor a segregação entre nossos clientes multilocatários e também entre o ambiente do cliente de serviço de nuvem e nossa própria rede interna.

2.1.4 Segurança do Perímetro

Em todos os perímetros entre a rede interna e uma rede externa (como a Internet), medidas efetivas devem ser tomadas para assegurar que apenas o tráfego de rede autorizado seja permitido. Isso geralmente consistirá em pelo menos um firewall de inspeção com informações de estado e, para os principais links com a Internet, um firewall de aplicativo (ou gateway de aplicativos) deve ser usado. Para conexões de banda larga em locais menores, um firewall de Filtragem de Pacotes pode ser suficiente, dependendo dos resultados de uma avaliação de risco.

Os servidores destinados a serem acessados a partir de uma rede externa e insegura (como servidores da Web) devem estar localizados em uma zona desmilitarizada (ZM) do firewall para fornecer proteção adicional à rede interna.

2.1.5 Redes Públicas

Onde a informação deve ser transferida através de uma rede pública como a Internet, uma criptografia forte via TLS deve ser usada para garantir a confidencialidade dos dados transmitidos.

Servidores que serão acessados a partir de dispositivos na rede pública estarão localizados na ZM do firewall.

2.1.6 Redes sem fio

As redes sem fio devem ser protegidas usando criptografia WPA2. WEP e WPA não devem ser usados.

As redes sem fio devem ser tratadas como inseguras, mesmo se o WPA2 for usado como o método de criptografia e um firewall instalado entre a rede sem fio e a LAN principal.

Uma rede sem fio para convidados pode ser fornecida para visitantes. Isso deve ser fisicamente separado de todas as redes internas (incluindo redes sem fio internas) e também protegido usando um firewall.

Os pontos de acesso sem fio devem ser configurados para não transmitir seu SSID e não permitir conexão segura usando o WPS (Wi-Fi Protected Setup) por meio do acesso físico ao próprio ponto de acesso.

As senhas de login do administrador do ponto de acesso sem fio sempre devem ser alteradas do padrão.

2.1.7 Segurança Física

Equipamentos de rede remota serão alojados em gabinetes seguros que serão trancados em todos os momentos. Somente a equipe de suporte terá acesso à chave de cada gabinete.

O backbone e o equipamento de rede centralizado serão alojados em gabinetes ou racks com chave apropriados em uma sala de servidores segura à qual somente a equipe de suporte autorizado terá acesso (com exceção da equipe de instalações locais por questões de saúde e segurança).

Pontos de acesso sem fio localizados em áreas públicas devem ser ocultados da vista quando possível e devem ser colocados em posições em que o acesso do público seja difícil, por exemplo. dentro ou perto do teto. Um invólucro de proteção com trava deve ser instalado onde um ponto de acesso está localizado em uma área pública desprotegida, por exemplo, em um estacionamento.

2.1.8 Acesso remoto

Onde houver um requisito para acesso remoto à rede interna, os seguintes controles serão usados:

- Uma rede virtual privada (VPN) será usada fornecendo criptografia de sessão usando SSL / TLS
- Autenticação de dois fatores no cliente, quando apropriado
- Autenticação segura usando um servidor RADIUS
- O Controle de Acesso à Rede (NAC) será usado para restringir o acesso a clientes remotos que não atendam aos requisitos mínimos. controle de vírus

O acesso remoto deve ser concedido conforme necessário e não para todos os usuários por padrão.

2.1.9 Detecção de Intruso na Rede

Um Sistema de Detecção de Intrusão baseado em Rede (NIDS) deve ser instalado no perímetro da rede e em todos os pontos chave dentro da rede, e em servidores críticos.

2.1.10 Padrões de Segurança de Rede

Os seguintes padrões serão adotados com relação à configuração e segurança da rede.

2.1.10.1 Hardware de rede

Sempre que possível, uma única política de fornecedor será usada para hardware de rede. Uma exceção será feita quando o uso de hardware de vários fornecedores puder aumentar o nível de segurança fornecido, por ex. em uma configuração de firewall baseada em rede dupla.

Roteamento de rede será baseado em roteadores Cisco usando OSPF. Os switches Cisco Gigabit serão usados como padrão para conectividade. As portas de switch, incluindo as portas de diagnóstico, serão configuradas para serem desativadas administrativamente até serem necessárias. Os hubs não serão usados devido a suas deficiências de segurança inerentes.

O Cat 6 UTP será usado para cabeamento de rede, a menos que circunstâncias específicas (como interferência excessiva) impeçam seu uso. A topografia de rede usada será Ethernet de acordo com a família de padrões IEEE 802.3.

2.1.10.2 Endereçamento IP

O IPv4 será usado em redes internas. No entanto, os novos dispositivos de rede adquiridos devem suportar o IPv6 em preparação para o futuro.

O intervalo de endereços IP interno usado será 192.168.0.0 - 192.168.254.254. a atribuição e o uso de sub redes devem ser monitorados cuidadosamente.

Endereços IP e informações de rede associadas para clientes de desktop e laptop serão controlados usando o DHCP. Servidores DNS internos serão usados.

2.1.10.3 Protocolos de Rede

O protocolo usado em todas as redes será o TCP / IP. O UDP será usado quando apropriado, mas outros protocolos de rede da camada 4 OSI não devem ser usados.

Somente protocolos e portas necessários em um servidor específico serão habilitados por padrão para reduzir a superfície de ataque. Isto é especialmente verdadeiro para servidores dentro da DMZ do(s) firewall(s).

2.2 Gerenciamento de Segurança de Rede

Uma vez que as redes tenham sido projetadas e implementadas com base em um conjunto claro de requisitos de segurança, há uma responsabilidade contínua de gerenciar e controlar o ambiente de rede seguro para proteger as informações da organização em sistemas e aplicativos. Isso deve ser alcançado por meio de controles nas seguintes áreas.

2.2.1 Funções e Responsabilidades

Papéis e responsabilidades pela gestão e controle de redes devem ser claramente definidos. A fim de proporcionar uma separação efetiva de tarefas, a operação das redes é gerenciada separadamente da operação do restante da infraestrutura, como servidores e aplicativos.

Essa segregação de funções é detalhada na tabela a seguir.

Função do gerente	Equipe	Responsabilidades Principais
Gerente de Redes	Gestão de Redes e Comunicações	Design e implementação de redes novas e alteradas Instalação e remoção de equipamentos de rede Configuração de equipamentos de rede Gerenciamento de incidentes de terceira linha
Gerente de Operações de Rede	Operações de Rede	Monitoramento de disponibilidade de rede Monitoramento de intrusão de rede Gerenciamento de incidentes de segunda linha Backups de configuração Patch e atualizações Configuração e gerenciamento de usuários de acesso remoto
Gerente de Operações de Computador	Operações de computador	Backups de servidor e aplicativo Agendamento de trabalho Monitoramento de Infraestrutura Gestão de incidentes de primeira linha

2.2.2 Registro e Monitoramento

Os níveis de registro em dispositivos de rede devem ser configurados de acordo com a política da organização e os registros monitorados regularmente.

Os logs de firewall serão monitorados em busca de sinais de varredura excessiva de portas, o que pode ser um precursor de um ataque remoto. Onde instalado, um sistema de detecção de invasões baseado em rede deve ser configurado para alertar a equipe de operações de rede sobre essa atividade.

O monitoramento de rede para disponibilidade pode ser obtido usando uma ferramenta de gerenciamento de rede baseada em SNMP e ações de recuperação automatizadas sempre que possível.

Os alertas do sistema Network Access Control (NAC) devem ser endereçados imediatamente para garantir que os clientes que não atendem aos requisitos mínimos de segurança tenham acesso permitido apenas a um subconjunto de sistemas em quarentena na rede.

2.2.3 Mudanças na Rede

Todas as alterações nos dispositivos de rede estarão sujeitas ao processo de gerenciamento de alterações e aos métodos adequados de avaliação de riscos, planejamento e retorno estabelecidos. Os registros de configuração devem ser atualizados sempre que tais mudanças forem executadas, de modo que uma imagem atual e precisa da rede seja mantida todo o tempo.

2.2.4 Incidentes de Segurança de Rede

Os eventos de rede que são considerados incidentes de segurança devem ser registrados e gerenciados de acordo com o Procedimento de Resposta a Incidentes de Segurança da Informação.

3 Conclusão

A segurança de rede é uma pedra angular das defesas da Cobmais contra muitas das ameaças com as quais nos deparamos. Somente projetando segurança efetiva em todos os novos sistemas e redes desde o início, o controle efetivo pode ser mantido e o risco reduzido. Além disso, controles adicionais devem ser implementados, garantindo que a segregação de funções seja alcançada e que as mudanças no ambiente de rede ocorram de maneira gerenciada.

Combinado com o monitoramento atento da própria rede e das ferramentas implementadas para gerenciá-la, isso deve garantir que o número e a gravidade dos incidentes de segurança de rede sejam minimizados e que nossa exposição daqueles que ocorrem não seja tão grande quanto de outra forma poderia ter sido.