Política de segurança de rede: White Paper de práticas recomendadas

Índice

Introdução

Sem uma política de segurança, a disponibilidade da sua rede pode ser comprometida. A política começa com a avaliação de risco da rede e com a formação de uma equipe de resposta. A continuação da política requer a implementação de uma prática de gerenciamento de alteração de segurança e a monitoração da rede em busca de violações de segurança. Por último, o processo de revisão modifica a política existente e a adapta às lições aprendidas.

Este documento é dividido em três áreas: preparação, prevenção e resposta. Vamos discutir em detalhes cada um destes passos.

Preparação

Antes de implementar uma política de segurança, você deve fazer o seguinte:

- Criar declarações de política de uso.
- Realizar uma análise de risco.
- Estabelecer uma estrutura de equipe de segurança.

Criar declarações de política de uso

Recomendamos criar declarações de política de uso que descrevam os papéis e responsabilidades dos usuários no que diz respeito à segurança. Você pode começar com uma

política geral que cubra todos os sistemas de rede e dados dentro da sua empresa. Este documento deve fornecer à comunidade geral de usuários uma compreensão da política de segurança, sua finalidade, diretrizes para melhorar suas práticas de segurança e definições de suas responsabilidades de segurança. Se sua empresa identificou ações específicas que poderiam levar a ações disciplinares ou punitivas contra um funcionário, essas ações e a forma de evitá-las devem ser articuladas de forma clara nesse documento.

O próximo passo é criar uma declaração de uso aceitável pelos parceiros para fornecer a eles uma compreensão das informações que estão disponíveis para eles, a disposição esperada dessas informações e a conduta dos funcionários da sua empresa. Você deve explicar claramente todos os atos específicos que foram identificados como ataques de segurança e as ações punitivas que serão tomadas se um ataque de segurança for detectado.

Por último, crie uma declaração de uso aceitável pelo administrador para explicar os procedimentos de administração de contas de usuário, imposição de políticas e revisão de privilégios. Se sua empresa possuir políticas específicas para senhas de usuário ou para a manipulação subsequente dos dados, apresente essas políticas de forma clara também. Verifique a política em relação ao uso aceitável por parceiros e declarações da política de uso aceitável pelos usuários para assegurar a uniformidade. Certifique-se de que os requisitos de administrador relacionados na política de uso aceitável sejam refletidos em planos de treinamento e em avaliações de desempenho.

Realizar uma análise de risco

Uma análise de risco deve identificar os riscos à sua rede, os recursos de rede e os dados. Isso não significa que você deve identificar cada possível ponto de entrada na rede, nem cada possível meio de ataque. A intenção de uma análise de risco é identificar áreas da sua rede, atribuir uma classificação de ameaça a cada área e aplicar um nível apropriado de segurança. Isso ajuda a manter um equilíbrio aceitável entre a segurança e o acesso necessário à rede.

Atribua a cada recurso de rede um dos seguintes três níveis de risco:

- Sistemas ou dados **de baixo risco** que, se comprometidos (exibição de dados por pessoas não autorizadas, dados corrompidos ou dados perdidos), não interromperiam as atividades comerciais nem causariam ramificações financeiras ou legais. O sistema alvo ou os dados podem ser facilmente restaurados e não permitem acesso adicional de outros sistemas.
- **Sistemas ou dados de médio risco** que, se comprometidos (exibição de dados por pessoas não autorizadas, dados corrompidos ou dados perdidos), causariam uma interrupção moderada nas atividades comerciais, pequenas ramificações financeiras ou legais ou forneceriam acesso adicional a outros sistemas. O sistema alvo ou os dados exigem um esforço moderado de restauração ou o processo de restauração causa interrupções no sistema.
- Sistemas ou dados de **alto risco** que, se comprometidos (exibição de dados por pessoas não autorizadas, dados corrompidos ou dados perdidos), causariam uma interrupção extrema das atividades comerciais, ramificações financeiras ou legais consideráveis ou ameaçariam a saúde e a segurança das pessoas. O sistema alvo ou os dados exigem esforço significativo para serem restaurados ou o processo de restauração causa interrupção nos negócios ou em outros sistemas.

Atribua um nível de risco a cada um dos seguintes itens: dispositivos de rede centrais, dispositivos de rede de distribuição, dispositivos de rede de acesso, dispositivos de monitoração

de rede (monitores de SNMP e sondas de RMON), dispositivos de segurança de rede (RADIUS e TACACS), sistemas de e-mail, servidores de arquivos de rede, servidores de impressora de rede, servidores de aplicações de rede (DNS e DHCP), servidor de aplicativos de dados (Oracle ou outros aplicativos autônomos), computadores desktop e outros dispositivos (servidores de impressora e equipamentos de fax de rede autônomos).

Os equipamentos de rede, tais como switches, roteadores, servidores DNS e servidores DHCP podem permitir acesso adicional à rede, e, consequentemente, são dispositivos de risco médio ou alto. Também é possível que o corrompimento deste equipamento poderia causar o colapso da própria rede. Uma falha desse tipo pode ser extremamente destrutiva para as atividades comerciais.

Uma vez que você atribuiu um nível de risco, é necessário identificar os tipos de usuários desse sistema. Os cinco tipos mais comuns de usuários são:

- Usuários internos **administradores** responsáveis pelos recursos de rede.
- Usuários internos **privilegiados** com necessidade de acesso adicional.
- Usuários internos com acesso geral.
- Usuários externos de **parceiros**com necessidade de acessos a alguns recursos.
- **Outros** usuários externos ou clientes.

A identificação do nível de risco e do tipo de acesso exigidos de cada sistema de rede forma a base da matriz de segurança a seguir. A matriz de segurança fornece uma referência rápida para cada sistema e um ponto de início para medidas de segurança adicionais, como a criação de uma estratégia apropriada para a limitação do acesso aos recursos de rede.

Sistema	Descrição	Nível de Risco	Tipos de Usuários
Switches ATM	Dispositivo de rede central	Alto	Administradores para a configuração de dispositivos (somente pessoal de suporte); Todos os outro para uso como um transporte
Roteadores de rede	Dispositivo de rede de distribuição	Alto	Administradores para a configuração de dispositivos (somente pessoal de suporte); Todos os outro para uso como um transporte
Switches de gabinete	Dispositivo de rede de acesso	Médio	Administradores para a configuração de dispositivos (somente pessoal de suporte); Todos os outro para uso como um transporte
Servid	Dispos	M	Administradores para a configuração

ores ISDN ou dial-up	itivo de rede de acesso	édio	de dispositivos (somente pessoal de suporte); Parceiros e usuários privilegiados para acesso especial
Guarda-fogo	Dispositivo de rede de acesso	Alto	Administradores para a configuração de dispositivos (somente pessoal de suporte); Todos os outro para uso como um transporte
Servidores DNS e DHCP	Aplicativos de rede	Médio	Administradores para a configuração; Usuários gerais e privilegiados para uso
Servidor de e-mail externo	Aplicativo de rede	Baixa	Administradores para a configuração; Todos os outros para o transporte de e-mails entre a Internet e o servidor de e-mail interno
Servidor de e-mail interno	Aplicativo de rede	Médio	Administradores para a configuração; Todos os outros usuários internos para uso
Banco de dados Oracle	Aplicativo de rede	Médio ou alto	Administradores para a administração do sistema; Usuários privilegiados para atualizações de dados; Usuários gerais para o acesso de dados; Todos os outros para o acesso a dados parciais

Estabelecer uma Estrutura de Equipe de Segurança

Crie uma equipe de segurança interfuncional liderada por um gerente de segurança com participantes de cada uma das áreas operacionais da sua empresa. Os representantes na equipe devem estar cientes da política de segurança e dos aspectos técnicos do design e da implementação da segurança. Frequentemente, isso exige treinamento adicional para os membros de equipe. A equipe de segurança possui três áreas de responsabilidade: desenvolvimento de políticas, prática e resposta.

O desenvolvimento de políticas visa estabelecer e revisar políticas de segurança para a empresa. No mínimo, revise anualmente a análise de risco e a política de segurança.

A prática é a fase durante que o equipe de segurança conduz a análise de risco, a aprovação da alteração de segurança pede, revê alertas de segurança de ambos os vendedores e da lista de endereços CERT, e transforma exigências da política de segurança do linguagem simples em aplicações técnicas específicas.

A última área de responsabilidade é a resposta. Enquanto a monitoração de rede frequentemente identifica violações de segurança, são os membros de equipe de segurança que fazem o troubleshooting e corrigem essas violações. Cada membro da equipe de segurança deve conhecer em detalhes os recursos de segurança fornecidos pelo equipamento em sua área operacional.

Enquanto nós definirmos as responsabilidades da equipe como um todo, você deve definir os papéis individuais e as responsabilidades dos membros de equipe de segurança em sua política de segurança.

Prevenção

A prevenção pode ser dividida em duas partes: aprovação das alterações de segurança e monitoração da segurança da rede.

Aprovando as alterações de segurança

As alterações de segurança são definidas como as mudanças no equipamento de rede que causam um possível impacto sobre a segurança total da rede. Sua política de segurança deve identificar requisitos de configuração de segurança específicos em termos não técnicos. Em outras palavras, em vez de definir uma exigência como “Nenhuma conexão de FTP de origens externas será permitido via firewall”, defina a exigência como da “Conexões externas não devem poder recuperar arquivos da rede interna”. Você precisará de definir um conjunto exclusivo de exigências para sua organização.

A equipe de segurança deve examinar a lista de exigências em linguagem simples para identificar a configuração de rede ou os problemas de desenho específicos que atendem às exigências. Uma vez que a equipe tenha criado as alterações de configuração obrigatórias da rede para implementar a política de segurança, você poderá aplicá-las a todas as futuras alterações de configuração. Ao mesmo tempo em que é possível para a equipe de segurança revisar todas as alterações, esse processo permite que eles examinem somente as alterações que representam risco suficiente para justificar o tratamento especial.

Recomendamos que a equipe de segurança examine os seguintes tipos de alterações:

- Qualquer alteração na configuração de firewall.
- Qualquer alteração nas listas de controle de acesso (ACL).
- Qualquer alteração na configuração do Simple Network Management Protocol (SNMP).
- Qualquer alteração ou atualização no software que difere da lista de nível de revisão do software aprovada.

Também recomendamos aderir às seguintes diretrizes:

- Mude as senhas dos dispositivos de rede rotineiramente.
- Restrinja o acesso aos dispositivos de rede a uma lista aprovada de pessoas.
- Assegure-se de que os níveis de revisão atuais do software do equipamento de rede e dos ambientes de servidor estejam em conformidade com os requisitos de configuração de segurança.

Além destas diretrizes de aprovação, envie um representante da equipe de segurança para participar da comissão de aprovação de gerenciamento de alterações a fim de monitorar todas as alterações revisadas pela comissão. O representante da equipe de segurança poderá recusar

qualquer alteração que seja considerada uma alteração de segurança até que ela seja aprovada pela equipe de segurança.

Monitoração da Segurança da Rede

A monitoração de segurança é similar à monitoração de rede, exceto que ela é voltada para a detecção de mudanças na rede que indicam uma violação de segurança. O ponto de início da monitoração de segurança determina o que é uma violação. Em Conduzir uma Análise de Risco, identificamos o nível de monitoração exigido baseado na ameaça ao sistema. Em Aprovação de Alterações de Segurança, identificamos ameaças específicas à rede. Ao examinar ambos esses parâmetros, desenvolveremos uma imagem clara do que você precisa monitorar e com que frequência.

Na matriz de análise de risco, o firewall é considerado um dispositivo de rede de alto risco, o indica que você deve monitorá-lo em tempo real. Na seção Aprovação de Alterações de Segurança, podemos ver que é necessário monitorar todas as alterações no firewall. Isso significa que o agente de polling SNMP deve monitorar aspectos como falhas de tentativas de login, tráfego incomum, alterações no firewall, acesso concedido ao firewall e conexões estabelecidas via firewall.

De acordo com este exemplo, crie uma política de monitoração para cada área identificada em sua análise de risco. Recomendamos monitorar o equipamento de baixo risco semanalmente, o equipamento de médio risco diariamente e o equipamento de alto risco de hora em hora. Se você necessitar de uma detecção rápida, monitore em um período de tempo mais curto.

Por último, sua política de segurança deve abordar a forma de notificar a equipe de segurança sobre as violações de segurança. Muitas vezes, seu software de monitoração de rede será o primeiro a detectar a violação. Ele deve acionar uma notificação para o centro de operações que, por sua vez, deve notificar a equipe de segurança usando um pager se necessário.

Resposta

A resposta pode ser dividida em três partes: violações de segurança, restauração e revisão.

Violações de segurança

Quando uma violação é detectada, a capacidade de proteger o equipamento de rede, determinar a extensão da intrusão e recuperar as operações normais dependem de decisões rápidas. Tomar essas decisões antes do tempo torna a resposta a uma intrusão muito mais gerenciável.

A primeira ação após a detecção de uma intrusão é a notificação da equipe de segurança. Sem um procedimento no lugar, haverá um atraso considerável para fazer com que as pessoas corretas forneçam as respostas adequadas. Defina um procedimento em sua política de segurança que esteja disponível 24 horas por dia, 7 dias por semana.

Em seguida, você deve definir o nível de autoridade atribuído à equipe de segurança para fazer mudanças e a ordem em que as mudanças devem ser feitas. As possíveis ações corretivas são:

- Implementar alterações para impedir acesso adicional à violação.
- Isolar os sistemas violados.
- Entrar em contato com a operadora ou o ISP para tentar rastrear o ataque.

- Usar dispositivos de gravação para recolher evidências.
- Desconectar os sistemas violados ou a fonte da violação.
- Entrar em contato com a polícia ou com outras agências do governo.
- Desligar os sistemas violados.
- Restaurar os sistemas de acordo com uma lista priorizada.
- Notificar o gerenciamento interno e a equipe jurídica.

Certificar-se de detalhar quaisquer alterações que possam ser conduzidas sem aprovação da gerência na política de segurança.

Finalmente, há duas razões para a coleta e manutenção de informações durante um ataque de segurança: determinar a extensão em que os sistemas foram comprometidos por um ataque de segurança e processar violações externas. O tipo de informação e a maneira como ela é coletada varia de acordo com seu objetivo.

Para determinar a extensão da violação, faça o seguinte:

- Grave o evento ao obter rastros de sniffers da rede, cópias dos arquivos de log, contas de usuário ativas e conexões de rede.
- Restrinja o comprometimento adicional da segurança ao desabilitar contas, desligar o equipamento de rede da rede e desconectar da Internet.
- Faça backup do sistema comprometido para auxiliar em uma análise detalhada dos danos e do método de ataque.
- Procure outros sinais de comprometimento. Muitas vezes, quando um sistema é comprometido, há outros sistemas ou contas envolvidos.
- Mantenha e examine os arquivos de log do dispositivo de segurança e os arquivos de log da monitoração da rede, pois frequentemente eles fornecem indícios do método de ataque.

Se você estiver interessado em tomar ações legais, peça ao seu departamento jurídico para examinar os procedimentos de coleta de evidências e de envolvimento das autoridades. Isso aumenta a eficácia da evidência nos procedimentos legais. Se a violação foi de natureza interna, entre em contato com seu departamento de recursos humanos.

Restauração

A restauração das operações normais da rede é o objetivo final de toda resposta de violação de segurança. Defina na política de segurança como você executa, protege e torna disponíveis backup normais. Como cada sistema possui seus próprios meios e procedimentos de backup, a política de segurança deve atuar como uma metapolítica, detalhando para cada sistema as condições de segurança que exigem a restauração do backup. Se houver necessidade de aprovação para que a restauração possa ser feita, inclua também o processo de obtenção da aprovação.

Revisão

O processo de revisão é o esforço final para criar e em manter uma política de segurança. Há três aspectos que você deve revisar: política, postura e prática.

A política de segurança deve ser um documento vivo que se adapta a um ambiente em constante mudança. Rever a política existente contra práticas recomendadas conhecidas mantém a rede atualizada. Também, verifique o site CERT para ver se há pontas, práticas, melhorias da Segurança, e alertas úteis que podem ser incorporados em sua política de segurança.

Você também deve examinar a postura da rede em comparação com a postura de segurança desejada. Uma empresa externa especializada em segurança pode tentar penetrar na rede e testar não somente a postura da rede, mas também a resposta de segurança da sua organização. Para redes de alta disponibilidade, recomendamos conduzir esse teste anualmente.

Finalmente, a prática é definida como um teste ou uma simulação do pessoal de suporte para garantir que eles possuem um entendimento claro do que a fazer durante uma violação de segurança. Frequentemente, essa simulação não é anunciada pelo gerenciamento e é feita em conjunto com o teste de postura da rede. Esta revisão identifica as lacunas entre os procedimentos e o treinamento da equipe para que a ação corretiva possa ser tomada.

Informações Relacionadas

- Mais Documentos de Práticas Recomendadas
- Suporte Técnico - Cisco Systems