1.Introdução à identificação de ameaças

1.1 Gerenciamento de configuração (control management)

O gerenciamento de configuração é uma prática em segurança da informação que se concentra na identificação, controle e manutenção de configurações de sistemas e software em uma infraestrutura. Envolve o estabelecimento de políticas, processos e ferramentas para gerenciar mudanças nas configurações, garantindo a integridade e segurança dos ativos de informação.

Os controles de resposta e recuperação referem-se a todo o conjunto de políticas, procedimentos e recursos criados para resposta e recuperação a incidentes e desastres. Esses controles são essenciais para a segurança cibernética, mas tornam-se cada vez mais difíceis de fornecer em grande escala. A resposta e a recuperação eficazes dependem muito de quão bem organizados estão os sistemas de TI no âmbito do site. Sem políticas organizacionais eficazes para administrar o gerenciamento de mudanças e configurações, a resposta e a recuperação são muito mais difíceis.

O controle e o gerenciamento de alterações reduzem o risco de que alterações nesses componentes possam causar interrupção do serviço. O ITIL (Information Technology Infrastructure Library) é um guia de boas práticas e processos para entrega de serviços de TI bastante utilizado, mundialmente falando. No ITIL, o gerenciamento de configuração é implementado usando os seguintes elementos:

- **Ativos de serviço:** São coisas, processos ou pessoas que contribuem para a entrega de um serviço de TI.
- **Item de configuração (IC):** É um ativo que requer procedimentos de gerenciamento específicos para ser usado na entrega do serviço. Cada IC deve ser identificado por algum tipo de rótulo, de preferência usando uma convenção de nomenclatura padrão. Cis são definidos por seus atributos e relacionamentos, que são armazenados em um banco de dados de gerenciamento de configuração (CMDB).
- **Configuração da linha base:** É o modelo de configurações para o qual um dispositivo, instância de VM ou outro IC foi configurado e que deve continuar a operar. Você também pode registrar linhas de base de desempenho, como o rendimento alcançado por um servidor, para comparação com os níveis monitorados.
- **Sistema de Gerenciamento de Configuração (CMS):** São as ferramentas e o banco de dados que coletam, armazenam, gerenciam, atualizam e apresentam informações sobre ICs e seus relacionamentos. Uma pequena rede pode

capturar essas informações em planilhas e diagramas; existem aplicativos dedicados para CMS corporativo.

- **Diagramas:** São a melhor maneira de capturar os relacionamentos complexos entre os elementos da rede. Os diagramas podem ser usados para mostrar como os ICs estão envolvidos nos fluxos de trabalho de negócios, topologias de rede lógica (IP) e física e layouts de rack de rede.

2.Gerenciamento de ativos

O Gerenciamento de Ativos de TI refere-se a um conjunto de práticas e processos que visam identificar, monitorar, manter e proteger os ativos digitais de uma organização. Esses ativos podem incluir hardware, software, dados, redes e outros componentes relacionados à infraestrutura de tecnologia. Um processo de gerenciamento de ativos rastreia todos os sistemas críticos, componentes, dispositivos e outros objetos de valor da organização em um inventário. Também envolve a coleta e análise de informações sobre estes ativos para que seja possível embasar alterações ou de outra forma trabalhar com ativos para atingir os objetivos de negócio da organização. Os principais aspectos do Gerenciamento de Ativos envolvem:

- **Identificação de ativos:** O processo começa pela identificação completa e precisa de todos os ativos de TI em uma organização. Isso inclui servidores, computadores, dispositivos de rede, software instalado, dados armazenados e outros elementos relacionados à infraestrutura de TI.
- **Classificação e categorização:** Após a identificação, os ativos são classificados e categorizados com base em critérios específicos, como importância operacional, criticidade para o negócio, riscos associados e outros parâmetros relevantes.
- **Monitoramento contínuo:** O gerenciamento de ativos envolve a implementação de ferramentas e práticas para monitorar continuamente o estado e o desempenho dos ativos. Isso pode incluir o rastreamento de alterações nas configurações, a detecção de vulnerabilidades de segurança e a avaliação do uso e da eficiência dos recursos.
- **Proteção e segurança:** O gerenciamento de ativos também abrange estratégias para proteger os ativos de TI contra ameaças de segurança. Isso envolve a implementação de políticas de segurança, criptografia de dados, controle de acesso e outras medidas destinadas a garantir a integridade, confidencialidade e disponibilidade dos ativos.
- **Manutenção e atualização:** Os ativos de TI precisam ser regularmente mantidos e atualizados para garantir seu desempenho otimizado e a conformidade com os requisitos de segurança. Isso inclui a aplicação de

patches de segurança, atualizações de software e manutenção preventiva de hardware.

- **Descarte adequado:** fim do ciclo de vida de um ativo também faz parte do gerenciamento de ativos. Isso envolve o descarte adequado de hardware obsoleto, a desativação segura de contas de usuários e a garantia de que dados confidenciais sejam adequadamente removidos antes da eliminação de ativos.

3.Controle de mudança

Um processo de controle de mudanças pode ser usado para solicitar e aprovar mudanças de forma planejada e controlada. As solicitações de mudança geralmente são geradas quando algo precisa ser corrigido, quando algo muda ou quando há espaço para melhorias em um processo ou sistema atualmente em funcionamento.

A necessidade de mudança é frequentemente descrita como reativa, onde a mudança é imposta à organização, ou como proativa, quando a necessidade de mudança é iniciada internamente. As alterações também podem ser categorizadas de acordo com o seu impacto potencial e nível de risco.

Em um processo formal de gerenciamento de mudanças, a necessidade ou os motivos da mudança e o procedimento para implementá-la são registrados em um documento de solicitação de mudança (RFC) e submetidos para aprovação.

A RFC será então apreciada no nível apropriado e as partes interessadas afetadas serão notificadas. Pode ser o supervisor ou gerente de departamento se a mudança for normal ou pequena. Mudanças importantes ou significativas podem ser gerenciadas como um projeto separado e exigir aprovação por meio de um conselho consultivo de mudanças (CAB).

Elementos Comuns de uma RFC são:

- **Descrição da mudança:** Detalhes claros e precisos sobre a natureza da mudança proposta, incluindo o que está sendo alterado, removido, ou adicionado.
- **Justificativa:** Uma explicação que fundamenta a necessidade da mudança. Isso pode incluir benefícios esperados, correção de problemas existentes, atendimento a requisitos regulatórios, entre outros.
- **Impacto da mudança:** Uma análise dos possíveis impactos da mudança, tanto positivos quanto negativos. Isso pode abranger áreas como operações, segurança, desempenho e custos.
- **Plano de implementação:** Um plano detalhado que descreve como a mudança será implementada, incluindo cronogramas, recursos necessários, testes a serem

realizados e procedimentos de reversão caso seja necessário desfazer a mudança.

- **Aprovação:** Um processo formal para a revisão e aprovação da RFC. Isso geralmente envolve uma equipe de gestão, um comitê de mudanças ou outras partes interessadas relevantes.
- **Documentação pós-implementação:** Após a implementação da mudança, a RFC pode ser atualizada para incluir informações pós-implementação, como resultados, lições aprendidas e qualquer ajuste adicional necessário.

4.Gerenciamento de mudanças (change management)

O gerenciamento de mudanças envolve uma série de processos destinados a planejar, avaliar, aprovar, implementar e validar mudanças em um ambiente organizacional. Os processos típicos de gerenciamento de mudanças podem variar dependendo do modelo específico de gerenciamento de serviços de TI adotado, como o ITIL.

Esses processos formam uma estrutura para garantir que as mudanças ocorram de maneira controlada, minimizando riscos e impactos adversos no ambiente operacional. Sua adoção promove a resiliência e a adaptabilidade de uma organização diante das mudanças necessárias em seus sistemas e serviços de TI.

A implementação das mudanças deve ser cuidadosamente planejada levando em consideração como a mudança afetará os componentes dependentes. Para mudanças mais significativas ou importantes, as organizações devem tentar acompanhar a mudança primeiro. Cada mudança deve ser acompanhada por um plano de reversão, para que as mudanças possam ser agendadas com cautela, se houver probabilidade de causar tempo de inatividade do sistema, ou outro impacto negativo no fluxo de trabalho das unidades de negócios que dependem do sistema de TI que está sendo modificado. A maioria das redes possui um período de janela de manutenção programada para tempo de inatividade autorizado.

Quando a mudança for implementada, o seu impacto deverá ser avaliado e o processo revisado e documentado para identificar quaisquer resultados que possam ajudar futuros projetos de gestão de mudanças. Abaixo estão os processos comuns associados ao gerenciamento de mudanças.

4.1 Identificação e registro de mudanças

Este processo envolve a identificação proativa de mudanças necessárias no ambiente de TI. Isso pode resultar de vários inputs, como melhorias identificadas, incidentes, ou requisitos de negócios. Suas atividades principais incluem: registro inicial da mudança, atribuição de um identificador único e documentação da descrição, justificativa e impactos iniciais.

4.2 Avaliação e análise de mudanças

Este processo visa avaliar as mudanças propostas quanto à sua viabilidade, impacto e riscos associados. Suas atividades principais incluem: análise de impacto, avaliação de riscos, revisão de custos e benefícios e definição de uma estratégia de implementação.

4.3 Aprovação de mudanças

Processo no qual as mudanças propostas são submetidas a uma revisão e aprovação formal antes de serem implementadas. As principais atividades incluem: apresentação da RFC para um comitê de mudanças ou gestores, revisão e avaliação da proposta, tomada de decisão sobre a aprovação.

4.4 Planejamento de mudanças

Este processo envolve a elaboração de um plano detalhado para implementar a mudança, considerando cronogramas, recursos necessários e procedimentos de reversão. As principais atividades são: desenvolvimento de um plano de implementação, estabelecimento de cronogramas e marcos, atribuição de responsabilidades.

4.5 Implementação de mudanças

A mudança é implementada conforme o plano desenvolvido, com monitoramento constante para garantir uma transição suave. As atividades principais incluem: execução do plano de implementação, monitoramento em tempo real, aplicação de procedimentos de reversão, se necessário.

4.6 Avaliação pós-implementação

Este processo envolve a avaliação dos resultados da mudança após a implementação, incluindo revisão de desempenho, feedback do usuário e identificação de lições aprendidas. As atividades principais são: coleta de dados pós-implementação, comparação dos resultados com os objetivos, documentação de lições aprendidas.

5.Defesa em profundidade

A segurança em camadas é normalmente vista como uma melhoria da resiliência da segurança cibernética porque fornece defesa profunda. A ideia é que, para comprometer totalmente um sistema, o invasor deve passar por vários controles de segurança, proporcionando diversidade de controle. Estas camadas reduzem a superfície potencial de ataque e tornam muito mais provável que um ataque seja dissuadido ou evitado, ou pelo menos detectado e depois evitado por intervenção manual.

A defesa em profundidade é uma estratégia que envolve a implementação de camadas múltiplas de segurança para proteger sistemas e dados. Em resiliência de site, isso significa que não se baseia em uma única linha de defesa, mas em várias camadas que precisam ser atravessadas antes que um ataque ou falha possa causar danos significativos. Os níveis de implementação podem ser:

- **Camadas de segurança:** Implementação de controles de segurança em várias camadas, incluindo firewall, antivírus, sistemas de detecção de intrusões, controle de acesso e criptografia, entre outros.
- **Monitoramento contínuo:** Monitoramento constante das operações do site para identificar atividades suspeitas ou falhas em tempo real. Isso permite uma resposta rápida a incidentes.
- **Atualizações e patches regulares:** Manutenção proativa dos sistemas, aplicando regularmente atualizações de segurança e correções de software para corrigir vulnerabilidades conhecidas.
- **Treinamento e conscientização:** Investimento em programas de treinamento para a equipe, garantindo que todos os membros compreendam e sigam as práticas de segurança. Isso reduz a probabilidade de erros humanos que podem levar a falhas.

6.Estratégias de engano

Um tipo de defesa ativa envolve a utilização de recursos chamariz para atuar como isca. É muito mais fácil detectar invasões quando um invasor interage com um recurso chamariz, porque você pode controlar com precisão o tráfego de linha de base e o comportamento normal de uma forma que é mais difícil de fazer para ativos de produção.

7.Honeypot

Um honeypot é um recurso de segurança projetado para ser alvo de ataques, desviando a atenção de sistemas reais. Existem dois tipos principais: honeypots de baixa interação, que emulam serviços sem expor vulnerabilidades reais, e honeypots de alta interação, que simulam sistemas operacionais completos e serviços reais. Ao atrair atacantes para um ambiente falso, os honeypots permitem que as organizações estudem táticas, técnicas e procedimentos (TTPs) de potenciais adversários. Isso facilita a detecção precoce e a resposta a ameaças reais.

7.1 Honeynet

Uma honeynet é uma rede de honeypots interconectados. Essa abordagem amplia as capacidades do honeypot, permitindo a observação de atividades coordenadas em uma escala maior. Honeynets proporcionam uma visão mais abrangente das estratégias de ataque, pois simulam uma rede real. Elas são

particularmente eficazes para a detecção de ataques coordenados e campanhas maliciosas mais amplas.

7.2 Honeyfile

Um honeyfile é um arquivo fictício projetado para atrair atividades maliciosas. Pode ser usado para detectar tentativas de acesso não autorizado a informações específicas. Ao monitorar e analisar atividades em torno do honeyfile, as organizações podem identificar tentativas de acesso não autorizado ou exfiltração de dados.

8.Estratégias de disrupção

A estratégia de interrupção, como parte das estratégias de defesa ativa, busca ativamente interromper ou perturbar as atividades maliciosas de um atacante para minimizar os danos e proteger os ativos da organização. Essa abordagem visa tornar mais difícil para os atacantes alcançar seus objetivos, desencorajando ou limitando seu progresso.

A interrupção pode ser aplicada em diferentes níveis, desde a camada de rede até a aplicação, e pode envolver a introdução de obstáculos, restrições ou respostas automáticas. Os principais componentes da estratégia de interrupção incluem:

- **Interrupção na camada de rede:** Identificação e bloqueio proativo de tráfego malicioso por meio de firewalls, sistemas de detecção de intrusões (IDS) e sistemas de prevenção de intrusões (IPS). Implementação de filtros de pacotes para bloquear endereços IP, portas ou padrões de tráfego associados a atividades maliciosas.
- **Interrupção na camada de sistema:** Suspensão ou restrição temporária de contas de usuário suspeitas ou comprometidas para impedir o acesso não autorizado. Identificação e encerramento de processos ou serviços maliciosos em execução no sistema.
- **Interrupção na camada de aplicação:** Implementação de soluções para mitigar ataques de negação de serviço distribuído (DDoS), como redirecionamento de tráfego ou filtragem de pacotes. Desativação temporária de funcionalidades ou serviços críticos que possam ser alvo de exploração até que uma solução mais abrangente seja implementada.
- **Resposta automatizada:** Desenvolvimento e implementação de scripts ou sistemas automatizados para responder rapidamente a eventos de segurança, como bloqueio automático de endereços IP ou isolamento de sistemas comprometidos.
- **Isolamento de segmentos de rede:** Isolamento de segmentos de rede suspeitos ou comprometidos para evitar a propagação lateral de um ataque. Desconexão

temporária de serviços ou servidores para evitar que o ataque se propague para outros sistemas.