Aplicação do NIST CSF

A estrutura CSF do NIST possui cinco funções principais: identificar, proteger, detectar, responder e recuperar.

Imagem: 5 funções principais doNIST CSF

Essas funções essenciais ajudam as organizações a gerenciar riscos de segurança cibernética, implementar estratégias de gerenciamento de riscos e aprender com erros anteriores. Os planos baseados nessa estrutura devem ser atualizados continuamente para se manter à frente das ameaças de segurança mais recentes. As funções essenciais ajudam a garantir que as organizações estejam protegidas contra potenciais ameaças, riscos e vulnerabilidades. Cada função pode ser usada para aprimorar a segurança de uma organização:

- **Identificar:**Gerencie riscos de segurança por meio de auditorias regulares de redes internas, sistemas, dispositivos e privilégios de acesso para identificar possíveis lacunas na segurança.
- **Proteger**:Desenvolva uma estratégia para proteger ativos internos por meio da implementação de políticas, procedimentos, treinamento e ferramentas que ajudem a mitigar ameaças à segurança cibernética.
- **Detectar**: Análise possíveis incidentes de segurança e melhore os recursos de monitoramento para aumentar a velocidade e a eficiência das detecções.

- **Responder**:Garantir que os procedimentos adequados sejam usados para conter, neutralizar e analisar incidentes de segurança e implementar melhorias no processo de segurança.
- **Recuperar**:Retorne os sistemas afetados à operação normal e restaure os dados e ativos dos sistemas que foram afetados por um incidente.

Algumas perguntas a serem feitas para cada uma das cinco funções principais, inclua:

Identificar	Crie um inventário de sistemas organizacionais, processos, ativos, dados, pessoas e capacidades que precisam ser protegidos: ● Tecnologia/Gestão de Ativos: Quais dispositivos de hardware, sistemas operacionais e softwares foram afetados? Rastreie o fluxo do ataque pela rede interna. ● Processo/Ambiente de negócios: Quais processos de negócios foram afetados no ataque? ● Pessoas: Quem precisa de acesso aos sistemas afetados?
Proteger	Desenvolver e implementar salvaguardas para proteger os itens identificados e garantir a prestação de serviços: ● Controle de acesso: Quem precisa ter acesso aos itens afetados? Como fontes não confiáveis são bloqueadas? ● Conscientização/Treinamento: Quem precisa ser informado sobre esse ataque e como evitar que ele aconteça novamente? ● Segurança de dados: há algum dado afetado que precisa ser mais seguro? ● Proteção de informações e procedimentos: É necessário atualizar ou adicionar algum procedimento para proteger os ativos de dados? ● Manutenção: Algum dos hardwares, sistemas operacionais ou softwares afetados precisa ser atualizado? ● Tecnologia de proteção: Há alguma tecnologia de proteção, como um firewall ou um sistema de prevenção de intrusão (IPS), que deve ser implementada para proteger contra ataques futuros?
Detectar	Projetar e implementar um sistema com ferramentas necessárias para detectar ameaça de ataques: ● Anomalias e eventos: Quais ferramentas podem ser usadas para

	detectar e alertar a equipe de segurança de TI sobre anomalias e eventos de segurança, como uma ferramenta de sistema de gerenciamento de informações e eventos de segurança (SIEM)? ● Monitoramento contínuo de segurança: quais ferramentas ou processos de TI são necessários para monitorar a rede em busca de eventos de segurança? ● Processo de detecção: Quais ferramentas são necessárias para detectar eventos de segurança, como um IDS?
Responder	Elabore planos de ação para responder a ameaças e ataques: ● Planejamento de resposta: Quais planos de ação precisam ser implementados para responder a ataques semelhantes no futuro? ● Comunicações: Como os procedimentos de resposta a eventos de segurança serão comunicados dentro da organização e com aqueles diretamente afetados pelo ataque, incluindo usuários finais e equipe de TI? ● Análise: Quais etapas de análise devem ser seguidas em resposta a um ataque semelhante? ● Mitigação: Quais medidas de resposta podem ser usadas para mitigar o impacto de um ataque, como colocar o sistema offline ou isolar os recursos afetados? ● Melhorias: Quais melhorias são necessárias para melhorar os procedimentos de resposta no futuro?
Recuperar	Elabore um plano e implemente a estrutura para recuperar e restaurar sistemas e/ou dados afetados: ● Planejamento de recuperação: como os recursos serão restaurados após um ataque? ● Melhorias: É necessário fazer alguma melhoria nos sistemas ou processos de recuperação atuais? ● Comunicações: Como os procedimentos de restauração serão comunicados dentro da organização e com aqueles diretamente afetados pelo ataque, incluindo usuários finais e equipe de TI?

O NIST CSF e suas cinco funções principais fornecem uma estrutura que permite o planejamento proativo para a aplicação de medidas reativas a ameaças à segurança cibernética. Essas funções são essenciais para garantir que uma organização tenha estratégias de segurança eficazes em vigor..Uma organização deve ter a capacidade de se recuperar rapidamente de qualquer dano causado por um incidente para minimizar seu nível de risco.