**Aplicação do CSF do NIST**

No início deste programa, você aprendeu sobre os usos e benefícios do National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). Há cinco funções principais da estrutura do NIST CSF: identificar, proteger, detectar, responder e recuperar.



*Imagem: 5 funções principais do NIST CSF*

Essas funções principais 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 principais ajudam a garantir que as organizações estejam protegidas contra possíveis ameaças, riscos e vulnerabilidades. Cada função pode ser usada para melhorar 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**: Desenvolver uma estratégia para proteger ativos internos por meio da implementação de políticas, procedimentos, treinamentos e ferramentas que ajudem a mitigar ameaças de segurança cibernética.
* **Detectar**: verifique 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 de volta 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, incluem:

|  |  |
| --- | --- |
| Identificar | Crie um inventário de sistemas, processos, ativos, dados, pessoas e recursos organizacionais que precisam ser protegidos:   * Gestão de Tecnologia/Ativos: Quais dispositivos de hardware, sistemas operacionais e software foram afetados? Rastreie o fluxo do ataque através da rede interna. * Processo/Ambiente de negócios: quais processos de negócios foram afetados no ataque? * Pessoas: Quem precisa ter 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 acessar os itens afetados? Como as fontes não confiáveis são impedidas de ter acesso? * Conscientização/Treinamento: Quem precisa ser conscientizado sobre esse ataque e como evitar que ele aconteça novamente? * Segurança de dados: há algum dado afetado que precisa ser tornado mais seguro? * Proteção de informações e procedimentos: algum procedimento precisa ser atualizado ou adicionado para proteger os ativos de dados? * Manutenção: algum dos hardwares, sistemas operacionais ou softwares afetados precisa ser atualizado? * Tecnologia de proteção: Existem tecnologias de proteção, como um firewall ou um sistema de prevenção de intrusão (IDS), que devem ser implementadas para proteger contra ataques futuros? |
| Detectar | Projetar e implementar um sistema com ferramentas necessárias para detectar ameaças e ataques:   * Anomalias e eventos: Quais ferramentas poderiam 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 eventos e informações 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 | Projetar 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 etapas de resposta podem ser usadas para mitigar o impacto de um ataque, como offlining ou isolamento de recursos afetados? * Melhorias: Que melhorias são necessárias para melhorar os procedimentos de resposta no futuro? |
| Recuperar | Construa 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 melhorias 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 de planejamento proativa para aplicar medidas reativas a ameaças de segurança cibernética. Essas funções são essenciais para garantir que uma organização tenha estratégias de segurança eficazes. Uma organização deve ter a capacidade de se recuperar rapidamente de qualquer dano causado por um incidente para minimizar seu nível de risco.