https://doi.org/10.6028/NIST.SP.1271pt

Introdução ao Framework de Segurança Cibernética do NIST: Um guia de iniciação rápida

Amy Mahn¹, Jeffrey Marron¹, Stephen Quinn², Daniel Topper³

- ¹ Divisão de Segurança Cibernética Aplicada do NIST, Laboratório de Tecnologia da Informação
- ² Divisão de Segurança de Computadores Aplicada do NIST, Laboratório de Tecnologia da Informação
- ³ Huntington Ingalls Industries



O que é o Framework de Segurança Cibernética do NIST e como a minha organização pode usá-lo?

O <u>Framework de Segurança Cibernética do NIST</u>⁴ é capaz de ajudar uma organização a começar ou a aprimorar seu programa de segurança cibernética. Criado com práticas reconhecidas e eficazes, ele pode ajudar as organizações a aprimorar sua postura em relação à segurança cibernética. Além de estimular a comunicação entre as várias partes interessadas envolvidas na segurança cibernética, tanto internas quanto externas, ele ajuda organizações maiores a integrar e alinhar o gerenciamento de riscos de segurança cibernética com processos empresariais mais amplos de gerenciamento de riscos, conforme descrito na série <u>NISTIR 8286</u>⁵.

O Framework é organizado em cinco funções principais: Identificação, Proteção, Detecção, Resposta e Recuperação. Esses cinco termos são amplamente conhecidos e, quando considerados em conjunto, oferecem uma visão abrangente do ciclo de vida do gerenciamento de riscos referentes à segurança cibernética ao longo do tempo. As atividades de cada função estão listadas abaixo e podem oferecer um bom ponto de partida para sua organização:

FRAMEWORK OF STANDARD OF STAND

IDENTIFICAÇÃO

Desenvolver uma compreensão organizacional para gerenciar os riscos de segurança cibernética referente a sistemas, ativos, dados e recursos.

• Identificar processos e ativos críticos da empresa

- Quais são as atividades que devem ter total continuidade para que a sua empresa seja viabilizada? Por exemplo, a manutenção de um site da Web para recuperar pagamentos, a proteção das informações de clientes/pacientes ou a garantia de que as informações coletadas pela sua empresa permaneçam acessíveis e precisas.
- Documentar fluxos de informações É
 importante não só entender quais tipos de
 informações sua empresa coleta e utiliza, mas
 também entender onde esses dados estão
 localizados e como são utilizados, especialmente
 no que envolve contratos e parceiros externos.

- Manter um inventário de hardware e software É importante conhecer os computadores e softwares da sua empresa, pois eles são os pontos de entrada de agentes maliciosos mais frequentes. Esse inventário pode ser algo simples como uma planilha.
- Estabelecer políticas para a segurança cibernética que incluam funções e responsabilidades – Essas políticas e procedimentos devem descrever claramente suas expectativas de como as atividades de segurança cibernética vão proteger suas informações e seus sistemas e como vão atender os processos críticos da empresa. As políticas de segurança cibernética devem ser integradas com outras considerações de risco da empresa (por exemplo, financeiras e reputacionais).
- Identificar ameaças, vulnerabilidades e riscos aos ativos – É preciso garantir que os processos de gerenciamento de riscos estejam estabelecidos e gerenciados para que ameaças internas e externas sejam identificadas, avaliadas e documentadas em registros de riscos. As respostas aos riscos devem ser identificadas, priorizadas e executadas e os seus resultados devem ser monitorados.

⁴ https://www.nist.gov/cyberframework

⁵ https://csrc.nist.gov/publications/detail/nistir/8286/final

PROTEÇÃO



Desenvolver e implementar as medidas de segurança adequadas para garantir a entrega dos serviços.

- Gerenciar o acesso a ativos e informações Crie contas exclusivas para cada funcionário e garanta que cada usuário tenha acesso às informações, aos computadores e aos aplicativos necessários para o trabalho. Autentique os usuários (por exemplo, com senhas e técnicas multifator) antes que eles tenham acesso a informações, computadores e aplicativos. Gerencie e monitore rigorosamente o acesso físico aos dispositivos.
- Proteger dados confidenciais Se a sua empresa armazena ou transmite dados confidenciais, verifique se esses dados estão protegidos por criptografia ao armazená-los em computadores e também ao transmiti-los para outras partes.
 Considere utilizar verificações de integridade para garantir que somente alterações aprovadas de dados sejam realizadas. Exclua ou destrua com segurança dados que não sejam mais necessários ou obrigatórios para fins de conformidade.

DETECÇÃO



Desenvolver e implementar as atividades adequadas para identificar a ocorrência de um evento de segurança cibernética.

◆ Testar e atualizar os processos de detecção – É preciso desenvolver e testar processos e procedimentos para detectar entidades e ações não autorizadas nas redes e no ambiente físico, incluindo atividades de pessoal. A equipe deve estar ciente de suas funções e responsabilidades quanto à detecção e às denúncias desse tipo de ação, seja dentro da sua organização ou perante o controle externo e autoridades jurídicas.

- Realizar backups regulares Muitos sistemas operacionais apresentam recursos integrados de backup; soluções de software e em nuvem também estão disponíveis para automatizar o processo de backup. Uma boa prática é manter um conjunto de dados com backup frequente offline para protegê-lo de ransomware.
- Proteger seus dispositivos Considere a instalação de firewalls baseados em hosts e de outras proteções, como produtos de segurança de endpoint. Aplique configurações uniformes aos dispositivos e controle as alterações em configurações de dispositivos. Desabilite os serviços ou recursos de dispositivos que não são necessários para atender as funções essenciais. Certifique-se de que haja uma política em vigor e que os dispositivos sejam descartados com segurança.
- Gerenciar vulnerabilidades de dispositivos –
 Atualize regularmente tanto o sistema operacional quanto os aplicativos instalados em seus computadores e em outros dispositivos para protegê-los de ataques. Se possível, habilite atualizações automáticas. Leve em consideração o uso de ferramentas de software para analisar os dispositivos em busca de vulnerabilidades adicionais; solucione as vulnerabilidades com alta probabilidade e/ou impacto.
- Treinar usuários Treine regularmente todos os usuários, mais de uma vez, para garantir que eles estejam cientes das políticas e dos procedimentos de segurança cibernética da empresa e das suas funções e responsabilidades específicas enquanto condição de trabalho.
- Conhecer os fluxos de dados esperados na sua empresa Se você souber quais e como são os dados esperados pela sua empresa, você terá uma probabilidade muito maior de perceber algo inesperado; e o inesperado nunca é bom quando se trata de segurança cibernética. Fluxos de dados inesperados podem incluir a exportação de informações de clientes de um banco de dados interno para a rede. Caso você tenha contratado um provedor de serviços gerenciado ou em nuvem, discuta com ele como será feita a monitoração de fluxos e relatórios de dados, incluindo os eventos inesperados.

• Manter e monitorar registros – Os registros são cruciais para identificar anomalias nos computadores e aplicativos de sua empresa. Esses registros documentam eventos como alterações de sistemas ou contas, assim como a iniciação de canais de comunicação. Considere o uso de ferramentas de software que possam agregar esses registros e buscar padrões ou anomalias em comportamentos esperados da rede.

FRAMEWORK

RESPOSTA

Desenvolver e implementar as atividades adequadas para agir durante a detecção de um evento de segurança cibernética.

- Garantir que os planos de resposta sejam testados
 - É ainda mais importante testar os planos de resposta para garantir que cada indivíduo conheça suas responsabilidades na execução do plano. Quanto melhor preparada a sua organização estiver, maior a probabilidade de uma resposta eficaz. Isso inclui o conhecimento de qualquer requisito legal de relatórios ou compartilhamento obrigatório de informações.
- Garantir que os planos de resposta estejam atualizados – Testar o plano (e a execução durante um incidente) inevitavelmente revelará a necessidade de melhorias. É preciso atualizar os planos de resposta com as lições aprendidas.

RECUPERAÇÃO



Desenvolver e implementar as atividades adequadas para manter os planos de resiliência e restaurar quaisquer recursos ou serviços afetados devido a um evento de segurança cibernética.

• Comunicar-se com partes interessadas internas e externas – Parte da recuperação depende de uma comunicação eficaz. Seus planos de recuperação devem levar em consideração cuidadosamente como, quando e quais informações serão compartilhadas com as diversas partes interessadas, de forma que todas elas recebam as informações necessárias, mas que nenhuma informação inadequada seja compartilhada.

• Entender o impacto de eventos de segurança cibernética –

Se um evento de segurança for detectado, sua empresa deve agir de forma rápida e cuidadosa para entender a amplitude e gravidade do impacto. Busque ajuda. Comunicar as informações sobre o evento com as respectivas partes interessadas vai deixá-lo em uma boa posição em termos de parceiros, órgãos de fiscalização e outros (incluindo, potencialmente, investidores), além de ajudá-lo a aprimorar políticas e processos.

• Coordenar com partes interessadas internas e externas – É importante se certificar de que os planos de resposta e as atualizações de sua empresa incluem todas as partes interessadas e os provedores externos de serviços. Eles podem contribuir com melhorias de planejamento e execução.



- Garantir que os planos de recuperação estejam atualizados – Assim como ocorre com os planos de resposta, testar a execução do plano aprimora a conscientização de funcionários e parceiros e destaca as áreas a serem melhoradas. É preciso atualizar os planos de recuperação com as lições aprendidas.
- Gerenciar relações públicas e a reputação da empresa – Um dos aspectos principais de recuperação é o gerenciamento da reputação da empresa. Ao desenvolver um plano de recuperação, considere como as relações públicas serão gerenciadas, de forma que o compartilhamento de informações seja preciso, completo e oportuno, não reativo.

