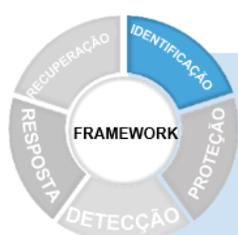


Introdução à gestão de risco de segurança cibernética | Ransomware

Guia de início rápido

Com a crescente ameaça de ransomware, este "guia de início rápido" ajudará as organizações a usar a **Gestão de risco de ransomware: Um perfil do Framework de segurança cibernética do NIST (National Institute of Standards and Technology) para combater ransomware**. Assim como o Framework de segurança cibernética do NIST, que é uma orientação voluntária amplamente utilizada para ajudar as organizações a melhor gerenciar e reduzir os riscos de segurança cibernética, o perfil de ransomware personalizado promove comunicações e ações baseadas em risco entre as partes interessadas internas e externas, incluindo parceiros e fornecedores.

O Framework é organizado em cinco funções principais: **Identificação, Proteção, Detecção, Resposta e Recuperação**. Esses cinco termos apresentam uma maneira abrangente de visualizar o ciclo de vida para gerenciar o risco de segurança cibernética. As atividades listadas em cada função oferecem um bom ponto de partida para qualquer organização, incluindo aquelas com recursos limitados para enfrentar os desafios da segurança cibernética. Elas ajudam a definir prioridades para que uma organização obtenha o maior valor de seus esforços para gerenciar os riscos de ransomware. Muito depende do nível de sofisticação das suas operações em termos de gestão de risco de segurança cibernética. Embora existam muitas outras ações que podem e devem ser feitas para combater o ransomware, é importante reconhecer que você não precisa fazer tudo de uma vez. *Começar é a chave na segurança cibernética, incluindo a gestão de risco de ransomware!* O NIST recomenda seguir estas etapas para ajudar a impedir o ransomware...



IDENTIFICAÇÃO

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

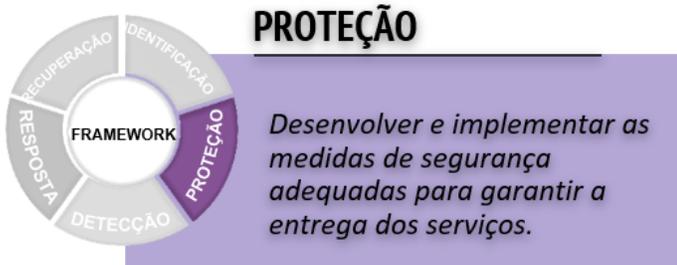
- ➔ **Manter inventários de hardware e software.** É importante entender qual hardware e software a sua empresa usa nos computadores. Esses são frequentemente os pontos de entrada de agentes maliciosos envolvidos em ataques de ransomware. Essas informações ajudam a corrigir vulnerabilidades que podem ser exploradas em ataques de ransomware e também são muito úteis na recuperação. Um inventário pode ser uma simples planilha. Os inventários de software devem identificar o nome e a versão do software, os dispositivos em que está instalado, a última data de correção e as vulnerabilidades conhecidas.
- ➔ **Documentar fluxos de informações.** Saber que tipo de informação sua empresa coleta e usa é essencial, assim como entender onde os dados estão localizados e por onde fluem, principalmente quando há contratos e parceiros externos envolvidos. Crie um registro de fluxos de informações (por exemplo, conexões entre dispositivos/endereços de protocolo de Internet) para

ajudar a enumerar quais informações ou processos estarão em risco se os invasores se moverem lateralmente em um ambiente.

- ➔ **Identificar os sistemas de informação externos aos quais sua empresa se conecta.** No caso de um evento de ransomware, você precisará planejar como se comunicar com os parceiros e identificar possíveis ações para se desconectar temporariamente dos sistemas externos. Identificar essas conexões também ajudará a implementar controles de segurança (por exemplo, direitos de acesso) e indicar áreas onde os controles podem ser compartilhados com terceiros.
- ➔ **Identificar os processos e ativos críticos da empresa.** Quais são as atividades que devem ter total continuidade para que a sua empresa seja viabilizada? Elas podem ser manutenção de um site para recuperar pagamentos, a proteção das informações de clientes/pacientes ou a garantia de que os dados coletados pela sua empresa permaneçam acessíveis e precisos. Essas informações são essenciais para entender o verdadeiro escopo e impacto dos eventos de ransomware. São essenciais também no planejamento de contingência para futuros eventos de ransomware, resposta a emergências e ações de recuperação. Ter essas informações com antecedência permite que as empresas priorizem os recursos. Se você depende de um sistema de controle industrial (ICS), inclua funções

críticas dele.

- **Estabelecer políticas de segurança cibernética que definem funções e responsabilidades.** Elas devem descrever claramente as expectativas de como as atividades de segurança cibernética da sua empresa, incluindo ações de funcionários, contratados e parceiros, protegerão suas informações e sistemas e atenderão aos processos empresariais críticos. As políticas de segurança cibernética devem ser integradas com outras considerações de risco da empresa (por exemplo, financeiras e reputacionais).



- **Gerenciar o acesso a ativos e informações.** Se você não fizer mais nada, limite o acesso a ativos físicos e relacionados a computadores e recursos associados a usuários, processos e dispositivos autorizados e gerencie o acesso de forma consistente com o risco de atividades e transações críticas.

Comece criando contas exclusivas para cada funcionário e garanta que os usuários tenham acesso apenas às informações, computadores e aplicativos necessários para seus trabalhos. Escolha contas de usuário padrão versus contas com privilégios administrativos sempre que possível. Autentique os usuários com senhas fortes ou técnicas multifatoriais antes que eles recebam esse acesso.

Como a maioria dos ataques de ransomware são realizados remotamente, controlar o acesso remoto é essencial para manter a integridade dos sistemas e arquivos de dados para proteção contra a inserção de código malicioso e a exfiltração de dados. Restrinja o acesso a redes oficiais de dispositivos pessoais. Gerencie e rastreie rigorosamente o acesso físico a dispositivos, seja um laptop ou um componente crítico de um sistema de controle industrial (ICS).

Em organizações maiores ou mais complexas, a segmentação ou segregação da rede pode limitar o escopo dos eventos de ransomware, impedindo que o malware se prolifere entre os sistemas que podem ser afetados. Isso é particularmente importante para funções críticas de ICS, incluindo Sistemas de instrumentos de segurança (SIS).

- **Gerenciar vulnerabilidades do dispositivo.** Atualize regularmente o sistema operacional e os aplicativos em seus computadores e outros dispositivos para protegê-los de ataques. *Mantenha-os totalmente corrigidos!* Se possível, habilite atualizações automáticas. Bloqueie o acesso a sites de ransomware. Leve em consideração o uso de ferramentas de software para analisar os dispositivos em busca de vulnerabilidades adicionais e solucionar as vulnerabilidades com alta probabilidade ou impacto. A configuração adequada dos processos de alteração e atualização pode ajudar a desencorajar a substituição de código por produtos que contenham malware ou não atendam às políticas de gestão de acesso.

- **Instruir e treinar funcionários e outros 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. Faça disso uma condição de trabalho. Treinar os responsáveis pela instalação, configuração e manutenção de hardware e software é fundamental, mas igualmente importante é treinar *todos os usuários* para sempre usar software antivírus, instalar somente se aprovado pela organização, clicar apenas em links verificados, conectar apenas a redes seguras e não conectar dispositivos a estações de carregamento públicas. Os usuários devem saber que seu acesso a redes oficiais de dispositivos pessoais é restrito. A maioria dos ataques de ransomware é possibilitada por usuários que se envolvem em práticas inseguras, administradores que implementam configurações inseguras ou desenvolvedores com treinamento de segurança insuficiente.

- **Proteger seus dispositivos com segurança.** 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 e uma maneira de descartar os dispositivos adequadamente. Essas medidas protegem contra a instalação de ransomware e também protegem contra vazamentos de dados.

- **Proteger dados confidenciais.** Sua organização provavelmente armazena ou transmite dados confidenciais, portanto, você deve gerenciar suas informações e registros (dados) de acordo com a sua estratégia de risco para proteger a confidencialidade, integridade e disponibilidade das informações. Use mecanismos de verificação de integridade (como assinaturas digitais) para verificar a integridade de

software, firmware e informações e detectar atualizações de software adulteradas que podem ser usadas para inserir malware.

- ➔ **Fazer backups regulares.** Garantir a disponibilidade de dados pode reduzir os impactos do ransomware. Isso inclui a capacidade de manter backups de dados fora do local e offline, bem como testar o tempo médio de recuperação e redundância do sistema. Muitos sistemas operacionais possuem recursos de backup integrados; software e soluções em nuvem também estão disponíveis para automatizar backups. É uma boa prática manter um conjunto de dados offline com backup frequente. Backups regulares mantidos e testados são essenciais para a recuperação oportuna e relativamente tranquila de eventos de ransomware. Proteja os backups e mantenha-os offline para que não sejam corrompidos ou excluídos por ransomware ou por um invasor.



DETECÇÃO

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

- ➔ **Testar e atualizar processos de detecção.** Desenvolva e teste processos e procedimentos para detectar eventos anômalos, como entidades e ações não autorizadas nas redes e no ambiente físico, incluindo atividade de pessoal. Isso inclui determinar o impacto de eventos que podem informar as prioridades de resposta e recuperação para um ataque de ransomware.

Organizações maiores ou mais complexas devem adquirir e instalar soluções de Gerenciamento de informações e eventos de segurança (SIEM) que incluam várias fontes e sensores para melhorar a visibilidade da rede, auxiliar na detecção precoce de ransomware e ajudar a entender como o ransomware pode se propagar pela rede. Essas ferramentas precisam gerar e registrar a atividade. Os registros são cruciais para identificar anomalias em computadores e aplicativos; eles registram eventos como mudanças em sistemas ou contas, bem como 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.

- ➔ **Treinar a equipe.** A equipe deve estar ciente de suas funções e responsabilidades para detectar ameaças e relatá-las para autoridades externas e da sua organização. Isso requer treinamento contínuo.
- ➔ **Conhecer os fluxos de dados esperados.** Se você souber quais e como são os dados que fluem 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 feito o monitoramento de fluxos e relatórios de dados, incluindo os eventos inesperados.

- ➔ **Comunicar rapidamente e determinar o impacto dos eventos de segurança cibernética.** A comunicação oportuna de eventos anômalos é essencial para a implementação de ações corretivas antes que um ataque de ransomware possa ser totalmente prejudicial. Se um evento de segurança cibernética for detectado, sua empresa deverá agir de forma rápida e cuidadosa para entender a amplitude e gravidade do impacto. Busque ajuda. A comunicação com as respectivas partes interessadas e autoridades (por exemplo, FBI) vai deixá-lo em uma boa posição perante parceiros, órgãos de fiscalização e outros (incluindo possíveis investidores), além de ajudá-lo a aprimorar políticas e processos.



RESPOSTA

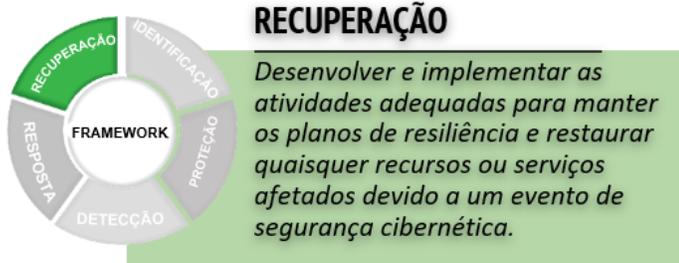
Desenvolver e implementar as atividades adequadas para agir durante a detecção de um evento de segurança cibernética.

- ➔ **Desenvolver planos de resposta.** Assim como em muitas outras esferas, a resposta a ransomware começa com o planejamento, incluindo a coordenação de planos com partes interessadas internas e externas. Concentre-se em procedimentos de mitigação imediata e contenção do evento de ransomware e na determinação do seu impacto.
- ➔ **Coordenar com as partes interessadas internas e externas.** Inclua todas as partes interessadas principais e os provedores de serviços externos. Mantenha uma lista prática e atualizada de contatos internos e externos para ataques de ransomware, incluindo autoridades,

assessoria jurídica e recursos de resposta a incidentes. As prioridades incluem mensagens preventivas e um acordo sobre como conter a disseminação de desinformação. As partes interessadas podem contribuir com melhorias de planejamento e execução.

- **Testar planos de resposta.** O teste ajuda a garantir que cada pessoa conheça suas responsabilidades na execução do plano. Quanto mais bem 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.
- **Atualizar planos de resposta.** Testar o plano (e executá-lo durante um incidente) inevitavelmente revelará a necessidade de melhorias. É preciso atualizar os planos de resposta com as lições aprendidas. Isso minimizará a probabilidade de futuros ataques de ransomware bem-sucedidos e ajudará a restaurar a confiança entre as partes interessadas.

- **Fazer planos de contingência.** Assim como a resposta, a recuperação de eventos de ransomware começa bem antes de um evento com planejamento de contingência. Nesse caso, sua empresa deve planejar a restauração dos recursos dos sistemas e a correção de vulnerabilidades. Concentre-se em procedimentos para mitigação imediata do evento de ransomware, determinando o impacto do evento e notificando as partes interessadas.
- **Comunicar-se com as partes interessadas internas e externas.** A recuperação depende de uma comunicação eficaz. Seus planos de recuperação precisam considerar cuidadosamente o que, como e quando as informações de eventos de ransomware serão compartilhadas com várias partes interessadas para que todas elas recebam as informações necessárias sem que nenhuma informação inadequada seja compartilhada.
- **Gerenciar as relações públicas e a reputação da empresa.** Ao desenvolver um plano de recuperação de ransomware, considere como as relações públicas serão gerenciadas, de forma que o compartilhamento de informações seja preciso, completo e oportuno, não reativo.
- **Testar e atualizar planos de recuperação.** Testar a execução dos planos de recuperação melhorará a conscientização dos funcionários e parceiros e destacará as áreas de melhoria. Sempre atualize os planos com as lições aprendidas.



ONDE ENCONTRAR MAIS RECURSOS DE RANSOMWARE DO NIST...

- ✓ **RECURSOS DE PROTEÇÃO E RESPOSTA:**
<https://csrc.nist.gov/projects/ransomware-protection-and-response>
- ✓ **SEGURANÇA CIBERNÉTICA DO NIST PARA PEQUENAS EMPRESAS:**
<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware>
- ✓ **PLANILHA DE DICAS E TÁTICAS:**
<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware>

PERGUNTAS? Envie-nos um e-mail: ransomware@nist.gov

Document translated courtesy of U.S. Department of State with support from the **Digital Connectivity and Cybersecurity Partnership (DCCP)**. Official U.S. Government Translation.

The official English language version of this publication is available free of charge from the National Institute of Standards and Technology (NIST):
<https://www.nist.gov/publications>.

Última atualização: Fevereiro de 2022