Criando uma Estratégia de Recuperação de Dados com Resiliência Virtual

Conteúdo

Introdução	**4**
História do NIST Cybersecurity Framework	**5**
Uma base confiável para a recuperação de dados	**8**
Função NIST "Identificar" (ID)	**9**
Catalogar sistemas e dados essenciais	**9**
Identificar e priorizar dados com marcação e classificação	**9**
Destacar lacunas e mudanças por meio de testes de recuperação automatizados	**9**
Função NIST "Proteger" (PR)	**10**
Uma infraestrutura de backup que não confia em ninguém	**10**
Analisar a conformidade da infraestrutura de backup	**10**
Garantir que os backups existam quando forem necessários	**11**
Criptografar seus próprios backups	**11**
Barra lateral: Modelo de segurança Zero Trust	**11**
Função NIST "Detectar"	**12**
Chamar atenção para comportamentos anormais	**12**
Verificar se há malware durante o backup	**12**
Detectar malware em backups	**12**
Testes regulares do plano de recuperação para detectar comprometimentos	**13**
Geração de relatórios e correlação centralizadas de registros	**13**
Integrações externas para proteção de dados	**13**
Barra lateral: Tempo de Permanência	**13**
Função NIST "Responder"	**14**
Usar backups para análises forenses virtuais	**14**
Caçada aprimorada às ameaças com o YARA	**14**
Acompanhamento de incidentes com o ServiceNow	**15**
Barra lateral: Exfiltração	**15**

Função NIST "Recuperar"	**16**
O backup só será útil se for restaurável (e não contiver malware)	**16**
Restaurar dados não infectados o mais rápido possível	**16**
Visualizar anomalias de E/S	**17**
Barra lateral: Backup x replicação para recuperação de cibersegurança	**17**
Função "Governar" do NIST	**18**
Certifique-se de que tudo esteja documentado	**18**
Monitor constantemente para minimizar os riscos	**19**
Painel de segurança do backup	**19**
Conclusão	**20**

Introdução

No mundo digital de hoje, a cibersegurança é uma necessidade fundamental. Não chega a surpreender que cada blog ou relatório de segurança cibernética que você lê hoje inevitavelmente gire em torno de ransomware. É cansativo ouvir falar (sabemos!), mas a ransomware se tornou a maior ameaça para organizações de todos os tamanhos e tem como alvo nossos setores mais críticos da indústria e infraestrutura. É um jogo de gato e rato e, à medida que novas ameaças surgem, as equipes de segurança devem se adaptar para acompanhar. A digitalização generalizada de operações de negócios, funções governamentais e atividades pessoais aumentou exponencialmente o volume de dados sensíveis armazenados e transmitidos online. Essa mudança, infelizmente, também ampliou a superfície de ataque para os cibercriminosos, o que torna medidas robustas de segurança cibernética essenciais.

As ameaças cibernéticas, que vão desde violações de dados e ataques de ransomware até espionagem cibernética sofisticada patrocinada pelo Estado, representam riscos significativos para a integridade da infraestrutura crítica, a privacidade das suas informações pessoais e até mesmo a estabilidade das economias globais. Portanto, a segurança de dados deve estar na linha de frente da estratégia de todas as organizações, pois a ameaça de ataques virtuais, principalmente o ransomware, é um perigo claro e presente. Infelizmente, 85% das empresas tiveram pelo menos um ataque ransomware em 2022[1]. O que é ainda mais alarmante é o fato de que os ataques de ransomware de hoje não estão apenas impedindo as organizações de acessar seus dados, eles estão exfiltrando, roubando, vendendo ou arquivando esses dados para uso em outros esquemas de extorsão.

Impedir o acesso malicioso a esses dados deveria ser a meta principal de qualquer plano de cibersegurança. Porém, nenhuma empresa deve supor que suas defesas resistirão sempre. Portanto, ter a capacidade de recuperar seus dados é igualmente importante. Nas organizações afetadas por ransomware, em média[2] 15% dos dados de produção foram perdidos, o que destaca a importância de ter um plano de recuperação de dados confiável e bem projetado.

Práticas eficazes de cibersegurança protegem contra o acesso não autorizado aos dados, garantem a continuidade das operações e mantêm a confiança entre consumidores e provedores de serviços. À medida que as ameaças cibernéticas evoluem em complexidade e escala, a importância da segurança cibernética para proteger os ativos digitais, proteger a privacidade individual e preservar a segurança nacional não pode ser subestimada. Isso é um pilar crítico na arquitetura da nossa sociedade digital e garante que possamos navegar, inovar e nos comunicar neste domínio com confiança.

A recente atualização para o NIST Cybersecurity Framework (CSF) 2.0[3] marca uma evolução fundamental na abordagem padrão da cibersegurança e reflete a mudança de paradigmas em um mundo em que as ameaças digitais são cada vez mais complexas e generalizadas.

Este artigo explora o NIST Cybersecurity Framework atualizado e discute os locais em que a Veeam Software pode ajudar na implementação desse framework.

[1] https://go.veeam.com/wp-data-protection-trends-2024

[2] https://go.veeam.com/wp-data-protection-trends-2024

[3] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

História do NIST Cybersecurity Framework

O NIST Cybersecurity Framework (CSF) foi introduzido pela primeira vez em 2014 em resposta à crescente necessidade de uma abordagem unificada para gerenciar riscos de segurança cibernética. A estrutura foi desenvolvida pelo National Institute of Standards and Technology (NIST) por meio da colaboração com entidades privadas e setor público e visava fornecer às organizações um conjunto de padrões para ajudar a proteger seus sistemas de informação. Os objetivos do CSF eram ajudar as organizações a compreender e melhorar a gestão do risco de cibersegurança, o que também aumentaria a segurança e a resiliência das infraestruturas críticas.

O NIST Cybersecurity Framework (CSF) 2.0, lançado em fevereiro de 2024, baseia-se nas versões anteriores e traz várias mudanças significativas que refletem a evolução do cenário de segurança cibernética e o feedback recebido da comunidade.

O CSF 2.0 estende seu alcance para além de setores de infraestrutura crítica, ele foi revisado para beneficiar todas as organizações, independentemente de tamanho ou tipo, o que torna essa diretriz mais universalmente aplicável.

Figura 1 — NIST Cybersecurity Framework 2.0

O núcleo do CSF está organizado em torno de seis funções principais e, quando consideradas em conjunto, essas características criam uma recomendação abrangente com base no ciclo de vida do risco de segurança cibernética.

- **Identificar:** Desenvolver um entendimento organizacional para gerenciar o risco de segurança cibernética para sistemas, pessoas, ativos, dados e recursos. Isso inclui identificar processos críticos de negócios e ativos-chave, além de suas vulnerabilidades e ameaças.
- **Proteger:** Implementar salvaguardas adequadas para garantir a prestação de serviços críticos e limitar ou conter o impacto de potenciais incidentes de cibersegurança. Isso inclui gerenciamento de identidade, controle de acesso, segurança de dados e tecnologia de proteção.
- **Detectar:** Implementar medidas para identificar a ocorrência de incidentes de cibersegurança em tempo hábil. O monitoramento contínuo e a detecção de ameaças são recursos importantes nesta função.
- **Responder:** Tome medidas quando um incidente de cibersegurança for detectado. Isso inclui planejamento da resposta, análise, mitigação e comunicação de incidentes.
- **recuperar:** Mantenha planos de resiliência e restauração de recursos ou serviços prejudicados por um incidente de cibersegurança. O objetivo é recuperação em tempo hábil para operações normais.
- **Governar (novo):** Esta nova função no CSF 2.0 centra-se na gestão geral e na governança do risco de cibersegurança. Aqui, as organizações estabelecem sua estratégia, políticas e supervisão de gerenciamento de riscos de segurança cibernética, incluindo a definição de funções e responsabilidades e a integração da segurança cibernética no gerenciamento de riscos empresarial.

A nova função "Governar" eleva os objetivos fundamentais de prestação de contas e transparência e serve como uma força de união para ajudar as organizações a priorizar e alcançar os objetivos delineados nas outras cinco funções. Ela também enfatiza que a segurança cibernética não é uma preocupação autônoma, mas parte integrante do que constitui risco empresarial. O componente de supervisão da nova função, em particular, ajuda as organizações a cumprir as estruturas regulatórias — como os regulamentos da SEC — que enfatizam o aumento da responsabilidade da alta administração e do Conselho de Administração ao fazer escolhas sobre segurança de TI.

Para melhorar a clareza e a relevância, as cinco funções originais — Identificar, Proteger, Detectar, Responder e Recuperar — foram mantidas e atualizadas para refletir a evolução das ameaças e práticas de cibersegurança, garantindo assim que as organizações possam gerenciar e reduzir efetivamente seus riscos de segurança cibernética em um ambiente digital dinâmico. Elementos relacionados à governança também foram transferidos para a recém-criada função "Governar". Além disso, os objetivos primordiais de cada função são agora mais claramente definidos. Ao reconhecer que estas tarefas não são sequenciais, mas sim partes interdependentes de uma estratégia de cibersegurança abrangente, esta reestruturação procura permitir uma abordagem mais coesa e ligada à cibersegurança.

O foco no gerenciamento de riscos da cadeia de suprimentos de segurança cibernética também está agora mais pronunciado, com novos controles destinados a integrar o gerenciamento de riscos da cadeia de suprimentos em todo o programa de segurança cibernética de uma organização.

Os usuários dessa estrutura agora recebem exemplos de implementação[4] e guias de início rápido[5] que também são adaptados às suas necessidades específicas. Isso inclui um catálogo pesquisável de referências[6], acessado por meio da ferramenta de referência, que permite que as organizações mapeiem orientações para mais de 50 outros documentos relevantes de segurança cibernética.

[4] https://www.nist.gov/document/csf-20-implementations-pdf

[5] https://www.nist.gov/quick-start-guides

[6] https://csrc.nist.gov/projects/olir/informative-reference-catalog#

As principais mudanças incluem:

1. O CSF 2.0 estende sua aplicabilidade para além dos setores de infraestrutura crítica. A estrutura revisada foi projetada para beneficiar todas as organizações, independentemente do tamanho ou do setor, tornando as diretrizes mais universalmente relevantes.
2. A adição da função "Governar" é um aprimoramento significativo no CSF 2.0. Essa função eleva os objetivos centrais de prestação de contas e transparência, ao mesmo tempo em que serve como uma força unificadora para ajudar as organizações a priorizar e atingir as metas delineadas nas outras cinco funções. Ele enfatiza a integração da segurança cibernética no gerenciamento de riscos corporativo como um todo, em vez de apenas tratá-la como uma preocupação autônoma. O componente de supervisão da função "Governar" é particularmente útil para as organizações em conformidade com estruturas regulatórias, como as regulamentações da SEC, que enfatizam o aumento da responsabilidade do conselho de administração e gerência sênior ao tomar decisões relacionadas à segurança cibernética.
3. Um foco maior na gestão de riscos da cadeia de suprimentos. O CSF 2.0 coloca uma ênfase mais forte no gerenciamento de riscos de cibersegurança na cadeia de suprimentos. Novos controles também foram introduzidos para integrar o gerenciamento de riscos da cadeia de suprimentos em todo o programa de segurança cibernética de uma organização. Isso reconhece a importância de proteger todo o seu ecossistema de parceiros, fornecedores e provedores de serviços.

Essas melhorias no NIST CSF 2.0 fornecem às organizações uma estrutura mais abrangente e adaptável para ajudá-las a navegar pelo cenário complexo da cibersegurança. Ao expandir o escopo, introduzir a função "Governar", atualizar as funções principais e enfatizar o gerenciamento de riscos da cadeia de suprimentos, o CSF 2.0 equipa as organizações com as ferramentas e orientações necessárias para fortalecer sua postura de segurança cibernética e construir resiliência diante de ameaças em evolução.

Os usuários dessa estrutura agora também recebem exemplos de implementação[7] e guias de início rápido[8] adaptados às suas necessidades específicas. Isso inclui um catálogo pesquisável de referências[9], acessado por meio da ferramenta de referência, que permite que as organizações mapeiem orientações para mais de 50 outros documentos relevantes de segurança cibernética.

[7] https://www.nist.gov/document/csf-20-implementations-pdf

[8] https://www.nist.gov/quick-start-guides

[9] https://csrc.nist.gov/projects/olir/informative-reference-catalog#

Uma base confiável para a recuperação de dados

A recuperação de dados, como parte de uma estratégia de disponibilidade de dados, muitas vezes é a parada final em um plano de segurança cibernética e, portanto, precisa ser bem considerada e planejada. Usar conceitos como uma estratégia de proteção de dados 3-2-1-1-0 e ter uma única ferramenta que possa fazer o backup dos dados em toda a infraestrutura e restaurá-lo para um estado íntegro após um incidente virtual dará às empresas uma configuração apropriada para recuperar dados em qualquer situação.

Figura 2 — Regra de backup 3-2-1-1-0 da Veeam

Com a Veeam Data Platform, os clientes da Veeam podem fazer tudo isso de maneira segura, orquestrada e bem documentada. Ao usarem o conjunto de software completo, que inclui o Veeam Backup & Replication, Veeam ONE e Veeam Recovery Orchestrator, os clientes podem cumprir objetivos de segurança de dados que se alinham com todos os estágios do NIST Cybersecurity Framework e ir muito além do backup e da recuperação de dados.

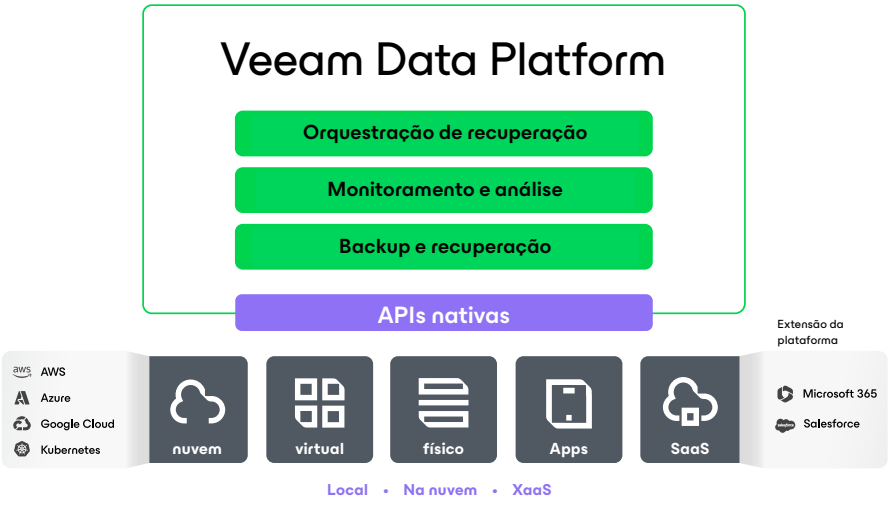

Figura 3 — Veeam Data Platform

Com referências constantes ao NIST Cybersecurity Framework abordado acima, o restante deste artigo tem o objetivo de fornecer a organizações de TI, equipes de segurança e tomadores de decisão os insights e conhecimentos necessários para usar efetivamente a plataforma de dados da Veeam dentro da estrutura. Também queremos fornecer a você outra rica fonte de informações e recursos que ajudam a identificar dados essenciais, detectar malware, proteger dados, responder rapidamente a ameaças ativas e recuperar rapidamente dados limpos, destacando os principais recursos que podem ser usados para alcançar esses objetivos.

Função NIST “Identificar” (ID)

Resultados desejados de cibersegurança:

Uma compreensão dos riscos atuais de cibersegurança da organização.

A cibersegurança compartilha um mantra muito importante com a recuperação de desastres (DR) tradicional: **você não pode proteger o que não conhece.** Catalogar e categorizar os ativos que precisam de proteção pode parecer desnecessário em comparação com o combate ativo e a reação a uma ameaça de cibersegurança, mas saber o que está em risco e sua prioridade relativa é o primeiro passo. Com os recursos a seguir, a Veeam pode se tornar parte essencial de uma estratégia multicamadas para **identificar** dados essenciais.

Catalogar sistemas e dados essenciais

Para criar um plano de recuperação confiável, as equipes de TI e segurança precisam trabalhar em conjunto com o restante da empresa para identificar, catalogar e priorizar todas as cargas de trabalho e dados que existem na organização. Um ótimo lugar para começar são os relatórios disponíveis no Veeam ONE e o catálogo de sistemas gravado em backup pelo Veeam Backup & Replication. Todos os dados essenciais devem ser gravados em backup, e a Veeam pode deixar claro se houver máquinas virtuais (VMs) ou dados que não estão sendo protegidos.

Da mesma forma, as ferramentas de rede e segurança usadas pela equipe de segurança podem criar uma lista de sistemas em seu ambiente. Comparar esses vários sistemas muitas vezes revelará onde os dados não estão protegidos de forma adequada em cada uma das ferramentas, garantindo que os planos de proteção e recuperação sejam os mais completos possível.

Identificar e priorizar dados com marcação e classificação

Ao utilizar os recursos de tagging e classificação de dados do Veeam Backup & Replication, os clientes podem começar com um catálogo existente de cargas de trabalho (seus backups) e aplicar tags para identificar metadados de sistema, como localização, proprietário e prioridade na recuperação. Às vezes, esse exercício destacará dados faltando, indicará uma lacuna na proteção de dados e identificará metadados importantes necessários para planejar adequadamente a recuperação de dados.

Quando os metadados são aplicados, o planejamento de recuperação orientado por assistente no Veeam Recovery Orchestrator pode ser usado para criar o plano de recuperação, reduzindo o tempo necessário para o desenvolvimento. Esse plano pode então ser analisado pela empresa como outra verificação, para garantir sua precisão e completude em relação às necessidades do negócio.

Destacar lacunas e mudanças por meio de testes de recuperação automatizados

A melhor maneira de identificar se um backup ou plano estará pronto para uso emergencial é testá-lo. Os recursos automatizados de testes do Veeam Recovery Orchestrator fornecem uma enorme vantagem para garantir a recuperabilidade completa de parte ou de toda a infraestrutura. Além das vantagens óbvias de redução de trabalho durante a execução do teste, automatizar o processo de teste de recuperação também pode significar testes mais frequentes, o que permitirá que eventuais falhas sejam identificadas mais rapidamente.

Uma das falhas que pode ser identificada com testes frequentes é quando os sistemas não estão sendo gravados em backup ou foram deixados de fora. Analisar regularmente os resultados dos testes e corrigir quaisquer lacunas melhorará o conhecimento da organização sobre o que precisa ser protegido.

Função NIST “Proteger” (PR)

Resultados desejados de cibersegurança:

Implemente salvaguardas para garantir a segurança de seus ativos.

A infraestrutura de backup é um lugar especial em qualquer ambiente de TI. Ela não apenas compõe a rede de proteção final da segurança de dados, mas também contém várias cópias de todos os seus dados (quanto mais críticos, mais cópias), incluindo dados que podem ter sido excluídos em produção. Isso a torna um alvo preferencial para os criminosos roubarem seus dados e comprometerem a segurança para aumentar a chance de sucesso dos seus esquemas de resgate e extorsão. É por isso que é essencial para você **Proteger** a sua própria infraestrutura de backup.

Uma infraestrutura de backup que não confia em ninguém

O primeiro passo para proteger os backups é impedir o acesso não autorizado ao sistema de gerenciamento de backup. Os princípios de Zero Trust — verificar explicitamente, presumir a violação e usar o acesso de menor privilégio — devem ser aplicados para dificultar ao máximo a movimentação lateral na infraestrutura de backup.

Usar a autenticação multifator (MFA) e ter um sistema separado e dedicado de proteção de dados de Identity and Access Management (IAM) garantirá que seus usuários e suas credenciais sejam verificados corretamente, dificultando seu comprometimento. Implementar o acesso de privilégios mínimos, como ter contas operacionais e de administrador separadas, também evitará erros não intencionais e minimizará o aumento de privilégios. Finalmente, tudo deve ser configurado partindo-se da premissa de que o resto da sua infraestrutura já foi comprometido. Isso significa isolar componentes de backup em uma rede separada e restringir o acesso ao console do Veeam Backup & Replication em si por meio de uma conexão VPN ou remota.

Cada nível da sua infraestrutura de backup deve incorporar essas abordagens, mas elas podem parecer ligeiramente diferentes em cada nível. Isso significa que os sistemas operacionais, compartilhamentos de arquivos, gerenciamento fora de banda e quaisquer aplicativos usados para gerenciá-los devem seguir princípios semelhantes.

Analisar a conformidade da infraestrutura de backup

Para ajudar os clientes a aplicar corretamente os princípios de Zero Trust, o console do Veeam Backup & Replication tem um utilitário integrado chamado “Analisador de conformidade e segurança” (anteriormente conhecido como “Analisador de melhores práticas”), que analisa a infraestrutura da Veeam e gera relatórios sobre itens de configuração que não foram implementados de acordo com nossas recomendações. Essa análise deve ser executada regularmente e cada um dos seus itens não conformes deve ser corrigido ou suprimido. Os itens suprimidos serão anotados com o usuário e a data/hora da supressão. Depois que a correção for concluída, a análise deve ser executada novamente e o resultado, documentado.

Garantir que os backups existam quando forem necessários

Excluir os backups para que os dados não possam ser recuperados agora é um recurso comum do ransomware. Portanto, garantir que os backups não possam ser modificados ou excluídos é crucial.

A imutabilidade é um conceito bem antigo na ciência da computação, que recentemente se tornou um recurso essencial para os backups, especialmente os backups que precisam permanecer sem mudanças ou erros para atender a requisitos de retenção. Se você usa repositórios seguros, storage de objetos, appliances de deduplicação de terceiros ou fita, os backups da Veeam podem ser armazenados em um estado em que nem mesmo os administradores poderão modificar ou excluir os dados. Assim como em qualquer sistema de segurança, muitas vezes há formas de contornar recursos, então é crucial considerar toda a pilha — até o piso do data center — para garantir que essas formas sejam eliminadas ou estritamente controladas.

É uma velha piada na cibersegurança que o sistema mais seguro é aquele que está desligado, desconectado da rede e armazenado em uma sala que ninguém pode acessar. Embora a piada seja completamente precisa, a verdade é que um sistema inacessível não tem razão de existir. Esse adágio, no entanto, pode funcionar bem na hora de considerar a segurança do backup. Desde que acessível, quando necessário, um backup armazenado off-line tem menos chances de ser adulterado. A Veeam fornece várias opções para criar essa abordagem de storage de backup isolado, desde sistemas online que exigem uma autenticação diferente até o storage offline definitivo: a fita.

Assim sendo, nenhum plano deve depender de apenas uma camada de proteção. Portanto, o Veeam Backup & Replication habilita o princípio dos "quatro olhos" para a exclusão do backup. Similar à antiga abordagem das "chaves nucleares", essa configuração exige que dois administradores autorizem a exclusão de um backup, protegendo os backups de exclusões acidentais ou maliciosas.

Criptografar seus próprios backups

Para proteger seus dados contra abusos após a exfiltração, a Veeam pode criptografar os backups para impedir que qualquer pessoa seja capaz de acessá-los fora da sua infraestrutura Veeam. Embora isso não impeça que seus dados sejam sequestrados ou bloqueados por meio de ransomware, tornará muito improvável que seus dados sejam usados como uma via para esquemas de extorsão. Essa criptografia pode ser gerenciada internamente pela Veeam ou vinculada a um sistema de gerenciamento de chaves (KMS) terceirizado para descarregar e centralizar o gerenciamento das chaves.

Barra lateral: Modelo de segurança Zero Trust

O objetivo do Zero Trust é eliminar a confiança natural que existe tradicionalmente na segurança de perímetro, reduzindo a capacidade das ameaças de se moverem facilmente por seu ambiente. Usar o lema "nunca confie, sempre verifique" cria um modelo de segurança sem perímetro que não presume que o firewall cuidará de deter as ameaças virtuais. Nesse modelo, cada sistema deve verificar cada nova interação e não fazer suposições de que elas são seguras. Os três princípios do modelo de segurança de confiança zero são:

1. **Verifique explicitamente.**

2. **Forneça o acesso de menor privilégio.**

3. **Presuma a violação.**

Função NIST "Detectar"

Resultados desejados de cibersegurança:

Desenvolver e implementar medidas apropriadas para identificar um evento de segurança cibernética.

Uma vez que o panorama total de sistemas e dados tiver sido identificado, a organização deve então estabelecer planos e sistemas para a detecção rápida de intrusões visando esses ativos. A detecção rápida reduzirá drasticamente o tempo de permanência e o impacto da ameaça, que geralmente pode se traduzir em dinheiro perdido. Aqui, a Veeam também pode ser um componente importante de uma estratégia multicamadas para **detectar** ameaças virtuais.

Chamar atenção para comportamentos anormais

Uma das principais estratégias do malware é evitar a detecção enquanto escala privilégios e se move lateralmente pelo ambiente, infectando o máximo possível de sistemas. Para conseguir isso, o malware pode fazer apenas pequenas alterações de cada vez para evitar ser detectado. Além disso, conforme se tornaram mais experientes em frustrar nossos esforços para recuperar os dados que desejam manter como reféns, os criadores de malware começaram a excluir os backups, reduzir os tempos de retenção dos backups ou desativar as tarefas de backup. A Veeam pode identificar e alertar você sobre esse tipo de comportamento anormal por meio de vários alarmes e relatórios do Veeam ONE.

Verificar se há malware durante o backup

Ao usar a detecção de malware em linha, o Veeam Backup & Replication pode analisar blocos à medida que eles passam pelos nós do Veeam Proxy em busca de sinais de criptografia nova, um indicador importante de atividade de malware. Com base em uma pesquisa do índice do backup, nomes de arquivos maliciosos e assinaturas serão detectados e, se algo suspeito for encontrado, o backup será marcado como suspeito.

Detectar malware em backups

O recurso SureBackup do Veeam Backup & Replication foi originalmente projetado para automatizar a restauração e a validação dos backups para garantir que eles sejam restauráveis. Como o software de proteção de endpoints não é perfeito, o que poderia levar à entrada do malware nos backups, o SureBackup também tem um conjunto robusto de recursos que podem verificar seus backups em busca de malware.

Como parte de um teste de viabilidade de restauração, o SureBackup também pode funcionar com ferramentas de detecção de malware para verificar sua máquina virtual (VM) restaurada. Isso dá às empresas a capacidade de usar uma segunda ferramenta de detecção de malware em uma abordagem de "confiar, mas verificar". Como vantagem adicional, a verificação do SureBackup ocorre sem nenhum impacto na carga de trabalho de produção, o que potencialmente permite uma verificação mais detalhada O SureBackup também pode montar discos individuais em uma máquina de testes, que pode então verificar os arquivos em busca de malware, fornecendo uma verificação ainda mais rápida e eficiente no uso de recursos sempre que uma restauração completa não for necessária.

Se algo for encontrado nessas varreduras, esse ponto de restauração específico será sinalizado como suspeito.

Testes regulares do plano de recuperação para detectar comprometimentos

Mais uma vez, testes regulares de plano de recuperação podem ser úteis, pois podem destacar a corrupção causada pelo malware. Falhas durante um teste completo de plano de recuperação, incluindo a verificação de aplicações, poderiam chamada a atenção para áreas em que um arquivo importante foi criptografado ou um arquivo de configuração foi modificado de forma inadequada. Isso pode ser especialmente útil na detecção de malware que é executado durante uma sequência de inicialização.

Geração de relatórios e correlação centralizadas de registros

Enviar arquivos de log para um serviço externo de syslog fornece um repositório secundário dos registros e uma centralização que permite correlacionar eventos entre sistemas. Essa é a função primária de um sistema de gerenciamento de incidentes e eventos de segurança (SIEM) para a maioria das equipes de segurança. Ao configurar o sistema SIEM como um destino de syslog, os indicadores de comprometimento descobertos pela Veeam podem ser marcados diretamente dentro do sistema, reduzindo o tempo de resposta e proporcionando aos analistas de segurança uma visão mais robusta dos eventos.

Integrações externas para proteção de dados

A API de Incidentes é um conjunto de interfaces de programação de aplicação (APIs) que as ferramentas de cibersegurança podem usar para informar à infraestrutura de backup sobre uma infecção e marcar os backups como suspeitos ou infectados. O Veeam Backup & Recovery pode ser configurado para alertar os administradores com base nessa informação, o que permite que eles analisem, verifiquem e respondam rapidamente com ações, como criar um backup imediato, executar uma ação do SureBackup para verificar infecções e recuperar arquivos limpos e criar uma cópia imutável do backup para fins de análise forense. Esse ponto aberto de integração entre as ferramentas principais de segurança e a plataforma de proteção de dados aprimora muito a comunicação, o que pode reduzir o tempo de latência do malware, levando a uma recuperação mais rápida e limpa.

Barra lateral: Tempo de Permanência

Tempo de latência — o tempo durante o qual o malware permanece no ambiente até ser descoberto. Ocorre enquanto o malware está dentro do ambiente sem desferir o ataque primário. Ele pode passar esse tempo comprometendo mais contas, escalando privilégios, incorporando-se mais profundamente ao seu sistema operacional, espalhando-se lateralmente para outros sistemas e coletando informações que podem ser usadas em ataques atuais ou futuros.

Função NIST "Responder"

Resultados desejados de cibersegurança:

Desenvolver e implementar reações apropriadas para um evento de cibersegurança detectado.

Não é possível estar sempre 100% protegido, então você também precisa se concentrar em parar o malware e removê-lo o mais rápido possível. Assim como no planejamento da recuperação de um desastre natural, um dos objetivos principais, ao qual todas as decisões devem estar alinhadas, é o objetivo de tempo de recuperação (RTO). Em um evento de segurança cibernética, há um objetivo muito semelhante que é focado em parar e remover seu malware do ambiente para que os sistemas possam ser reativados em serviço. Ser capaz de reduzir o tempo que o malware terá para habitar e exfiltrar seus dados reduzirá o esforço de limpeza e melhorará tempo de recuperação, e é por isso que é fundamental se preparar para **responder** rapidamente.

Usar backups para análises forenses virtuais

Conforme discutido anteriormente, o SureBackup é uma funcionalidade que não só testa a restauração do backup, mas também pode detectar malware. Um dos objetivos na fase de resposta é identificar o tempo de latência. Usar indicadores de malware no Veeam Backup & Replication, que indicam se o malware foi detectado em um ponto de restauração ou encontrado por uma ferramenta de terceiros, facilita a busca necessária para encontrar o primeiro ponto de infecção.

A restauração segura é outra função do Veeam Backup & Replication que permite que os discos sejam montados e verificados em busca de malware antes da restauração completa. Iterar esse processo até que um ponto não infectado seja descoberto facilita encontrar o momento no tempo em que o malware apareceu pela primeira vez em um determinado sistema e ajuda a evitar a reinfecção restaurando um malware dormente.

Com o Veeam Recovery Orchestrator, esse processo de restauração segura pode ser executado no ambiente inteiro, em uma abordagem orquestrada de "sala limpa". Isso não só adiciona velocidade à busca de pontos de restauração limpos, mas também pode acrescentar rapidamente informações valiosas às análises forenses digitais de um incidente de cibersegurança.

Caçada aprimorada às ameaças com o YARA

O YARA é uma ferramenta conhecida pelos caçadores de ameaças de cibersegurança e usa uma abordagem baseada em regras para identificar e classificar malwares. Como parte de uma operação do SureBackup ou de restauração segura, uma regra do YARA pode ser identificada e executada para a classificação inicial do malware e, em seguida, para procurá-lo nos backups.

Acompanhamento de incidentes com o ServiceNow

Com integrações diretas com o ServiceNow, a Veeam ONE pode criar automaticamente casos novos e atualizar os existentes conforme a situação evolui, ajudando equipes diferentes a se comunicar de modo mais eficiente e fornecendo uma documentação mais automatizada do histórico do incidente.

Barra lateral: Exfiltração

Se os dados foram acessados e modificados por malware, é provável que tenham sido roubados primeiro. Dados exfiltrados são aqueles enviados do ambiente da vítima para os criminosos virtuais. Eles podem se tornar informações divulgadas ou vendidas por cibercriminosos após uma violação, o que pode causar a exposição de segredos corporativos, danos a reputações e roubo de informações pessoais, que, por sua vez, podem levar a fraudes ou ataques cibernéticos futuros.

Função NIST "Recuperar"

Resultados desejados de cibersegurança:

Desenvolver e implementar as atividades apropriadas para recuperar de um evento de segurança cibernética (planos, processo, pessoas, tecnologia)

Dependendo da natureza do seu incidente de cibersegurança, restaurar dados limpos será crucial para colocar os serviços online novamente, especialmente com ransomware. Se o tempo de latência for longo, então muitos pontos de restauração podem conter malware e pode haver a necessidade de voltar muito no tempo para encontrar um ponto de restauração limpo. Assim como na recuperação de desastres tradicional, é importante alinhar objetivos que minimizem a perda de dados: Seus objetivos de ponto de recuperação (RPOs). Como é importante descobrir o início da infecção na fase de resposta, muitos desses esforços ocorrerão em paralelo com os esforços para **recuperar** seus dados.

O backup só será útil se for restaurável (e não contiver malware)

A marcação de pontos de restauração suspeitos ou infectados durante as fases de detecção e resposta, feita por recursos como o SureBackup e a API de incidentes, torna muito fácil identificar diretamente no console do Veeam Backup & Replication se houve detecção de malware em cada ponto de restauração. Esse é um ótimo ponto de partida, mas não garante que os pontos de restauração mais antigos estejam completamente limpos.

Para reduzir as chances de restaurar dados infectados e desperdiçar esforços, os esforços de recuperação devem trabalhar em conjunto com as análises forenses cibernéticas que ocorrem na fase de resposta. Uma forte parceria de trabalho entre a TI, a segurança e a empresa como um todo é essencial para restaurar os dados certos e não reintroduzir o malware.

Malware não detectado anteriormente pode ser encontrado em pontos de restauração mais antigos tquando você utiliza ferramentas de detecção de malware totalmente atualizadas como parte do SureBackup e da restauração segura. Por isso, é importante não depender apenas de flags de malware das verificações iniciais. Caso os pontos de restauração limpos sejam mais antigos do seus RPOs definidos restaurações no nível do arquivo poderão ser usadas para restaurar dados importantes individuais, evitando o malware contido no backup completo.

Restaurar dados não infectados o mais rápido possível

A automação é essencial para recuperar rapidamente até o mais simples dos ambientes, mas o modo de restauração também pode fazer a diferença. Com a ajuda de snapshots de storage array e recuperação instantânea, os backups restaurados podem ser usados quase que instantaneamente.

O Veeam Recovery Orchestrator foi projetado para definir todo o processo de restauração e torná-lo tão simples quando clicar em um único botão. Ao combinar o plano de restauração com flags de infecção, restauração segura, snapshots de storage array, recuperação instantânea e verificação de aplicativos, a Veeam oferece uma coleção de recursos capaz de restaurar dados de forma rápida e eficiente, além de garantir que os dados estejam tão livres de malware quanto possível.

Visualizar anomalias de E/S

Às vezes, nada destaca uma tendência melhor do que um gráfico visual. Na interface de usuário do Veeam Backup & Replication, gráficos são fornecidos na recuperação a partir de um job de replicação para ajudar a identificar o momento em que a criptografia em massa começou, reduzindo assim o esforço necessário para encontrar um momento no tempo anterior à criptografia.

Barra lateral: Backup x replicação para recuperação de cibersegurança

A replicação pode fazer parte do seu plano de recuperação de cibersegurança, mas é importante compreender os objetivos da replicação em comparação com os backups. A replicação serve para mover dados o mais rápido possível e retorná-los para a réplica íntegra mais recente. Os backups não são contínuos e, portanto, podem ser mais metódicos ao garantir a limpeza e a restauração. A recuperação de cibersegurança deve ser baseada no tempo de latência e na limpeza do ponto de restauração, o que tornará os backups um mecanismo mais comum.

Função "Governar" do NIST

Resultados desejados de cibersegurança:

A estratégia de gerenciamento de riscos de segurança cibernética, as expectativas e a política da organização são estabelecidas, comunicadas e monitoradas.

A introdução da função "Governar" representa uma evolução significativa na estratégia e supervisão de segurança cibernética. Essa nova função enfatiza a importância da governança no gerenciamento do risco de segurança cibernética em toda a organização. Ele também ressalta a necessidade de estabelecer políticas, estratégias e processos claros de segurança cibernética que estejam alinhados com os objetivos gerais e a tolerância ao risco da sua organização. Ao integrar a função "Governar", o NIST CSF 2.0 incentiva as organizações a adotarem uma abordagem mais holística e responsável em relação à segurança cibernética, garantindo assim que as considerações de segurança cibernética sejam incorporadas à estrutura da governança organizacional. Isso inclui definir papéis e responsabilidades para a cibersegurança, promover uma cultura de conscientização de segurança e garantir que as decisões de segurança cibernética sejam informadas por objetivos e restrições organizacionais. A adição dessa função destaca a mudança em direção ao reconhecimento da segurança cibernética não apenas como um desafio técnico, mas como um componente crítico da gestão de negócios e da resiliência operacional.

Como um componente essencial da segurança dos dados, sua infraestrutura de backup precisa estar comprovadamente em conformidade com as regulamentações da empresa e governamentais. "**Governar**" corretamente inclui a documentação da estratégia de gerenciamento de risco de segurança cibernética da sua empresa, incluindo configuração e políticas, controle de alterações e documentar os sucessos e fracassos de cada teste. Isso ajuda a garantir que as expectativas e as políticas sejam efetivamente comunicadas e monitoradas.

Certifique-se de que tudo esteja documentado

Seja para auditores, seguro cibernético, melhoria de processos ou autoconfiança, a importância de uma documentação precisa, completa e frequente não pode ser superestimada. A precisão e a velocidade de um plano de recuperação totalmente orquestrado oferecerão o maior valor para administradores e proprietários de empresas, mas a documentação dinâmica criada a cada execução completa ou de teste será de grande valor para qualquer equipe que precise de evidências de que a recuperação realmente funcionou, incluindo equipes de segurança e conformidade.

Além disso, o número de relatórios possíveis no Veeam ONE fornecerá uma grande quantidade de informações sobre sua infraestrutura de backup e sua saúde. Documentar a frequência dos backups, controle de alterações para configurações de backup e outros são relatórios integrados que podem ser gerados manualmente ou em um cronograma e então enviados automaticamente para os destinatários corretos.

Monitor constantemente para minimizar os riscos

Utilize automação para verificar as configurações da Veeam e o ambiente de backup a fim de garantir que seus dispositivos e software estejam seguros e atualizados. Com o Veeam Security and Compliance Analyzer, a Veeam realiza automaticamente 30+ verificações de segurança para garantir que você esteja atualizado, em dia com os patches e que seus protocolos antigos e inseguros estejam desativados. Além disso, todas essas informações são compiladas em um único relatório para que as equipes de segurança e TI acompanhem a aderência às políticas da organização.

Painel de segurança do backup

A segurança cibernética geralmente envolve encontrar padrões em todo o seu ambiente. A Veeam oferece uma ampla variedade de recursos, incluindo novos recursos focados na cibersegurança, como o painel do Veeam Threat Center, um painel único que agrega múltiplas fontes de dados na interface do Veeam ONE e fornece aos administradores e especialistas em segurança uma visão única de toda a sua infraestrutura de backup.

Conclusão

O NIST CSF 2.0 representa um marco significativo na evolução da gestão de riscos de cibersegurança e na luta contra a evolução das ameaças. Ao se basear nos fundamentos sólidos do CSF 1.1 e introduzir melhorias importantes como a função "Governar" e um foco maior na cadeia de suprimentos, o CSF 2.0 fornece às organizações uma estrutura mais abrangente e adaptável para ajudá-las a navegar em seu cenário de segurança cibernética em constante mudança.

O escopo expandido do CSF 2.0 garante que organizações de todos os tamanhos e setores possam se beneficiar de suas orientações, promovendo assim uma abordagem mais inclusiva e colaborativa para a segurança cibernética. A estrutura atualizada também reconhece que um gerenciamento eficaz de riscos de segurança cibernética requer o envolvimento ativo e o comprometimento das partes interessadas em toda a organização, desde executivos seniores até funcionários da linha de frente.

Em última análise, o sucesso da implementação do NIST CSF 2.0 depende da promoção de uma cultura de conscientização, colaboração e responsabilidade sobre segurança cibernética. Ao investir em programas de treinamento e educação, as organizações podem capacitar sua força de trabalho para se tornarem participantes ativos no processo de gerenciamento de riscos de segurança cibernética. Uma comunicação clara e um reforço consistente das políticas e melhores práticas de cibersegurança são essenciais para criar um sentido partilhado de responsabilidade e vigilância.

À medida que olhamos para o futuro, é evidente que a segurança cibernética continuará a ser uma prioridade crítica para as organizações em todo o mundo. A crescente sofisticação e frequência das ameaças cibernéticas, juntamente com a dependência cada vez maior das tecnologias digitais, ressaltam a necessidade de estruturas de segurança cibernética robustas e ágeis, como o NIST CSF 2.0. Ao adotarem essa estrutura atualizada e se comprometerem com sua implementação contínua, as organizações podem fortalecer sua resiliência, proteger seus ativos e manter a confiança de suas partes interessadas diante da evolução dos riscos cibernéticos.

Criar um programa de cibersegurança não é uma tarefa fácil hoje em dia. As ameaças são muitas e o valor de uma violação para os criminosos é potencialmente enorme. Por isso, as empresas precisam usar todas as ferramentas à sua disposição para criar camadas de segurança de modo a maximizar sua eficácia em todos os estágios do NIST Cybersecurity Framework. A Veeam pode agregar valor a todos os estágios do NIST Cybersecurity Framework, melhorando o programa geral de cibersegurança da empresa:

- O ato de criar e testar regularmente os planos de recuperação pode fornecer dados valiosos que você pode usar na fase de identificação para garantir que dados essenciais sejam **identificados** e possam ser protegidos.
- Implementar as melhores práticas documentadas e recursos nativos de segurança garantirá que os backups e a infraestrutura de backup sejam tratados na fase **Proteger**.
- Como os backups incluem todos os dados da infraestrutura, eles podem atuar como uma segunda verificação importante para encontrar malware que talvez tenha sido ignorado nas observações de endpoint, na fase **Detectar**.
- O acesso rápido a diferentes pontos no tempo e ambientes virtuais de "sala limpa" pode ser essencial para as iniciativas de coleta de informação na fase **Responder**.
- Os backups comprovadamente restauráveis e livres de malware estarão disponíveis quando necessário e poderão ser restaurados em um estado limpo e utilizável o mais rápido possível para possibilitar a fase **Recuperar**.
- Todos desempenham um papel na proteção de suas organizações e de seus dados. Estabelecer, comunicar e monitorar a estratégia e as políticas de segurança cibernética da sua organização é fundamental na fase "**Governar**".

Já é hora das equipes de TI deixarem de ser simples guardiões de dados restauráveis e se tornarem participantes ativas no plano de cibersegurança. Usando as orientações desse documento, as equipes de TI agora devem ser capazes de manter uma conversa produtiva com as equipes de cibersegurança e partes interessadas da organização para integrar uma plataforma de proteção de dados baseada na Veeam ao seu programa geral de cibersegurança.

Entre em contato conosco para mais detalhes sobre as funcionalidades e recursos da Veeam.

Sobre a Veeam Software

A Veeam, líder Nº 1 do mercado global em proteção de dados e recuperação de ataques de ransomware, tem a missão de capacitar todas as organizações a alcançar a resiliência radical com segurança, recuperação de dados e liberdade de dados para suas nuvens híbridas. Com sede em Seattle e escritórios em mais de 30 países, a Veeam protege mais de 450.000 clientes em todo o mundo que confiam na Veeam para manter seus negócios em operação. Saiba mais em www.veeam.com ou siga a Veeam no LinkedIn @veeam-software e no X @veeam.

→ Assista à Veeam Data Platform em ação

→ Experimente gratuitamente por 30 dias