SOPHOS

Guia de Planejamento e Resposta a Incidentes da Sophos

Índice

Introdução

Este documento foi escrito para oferecer uma visão abrangente das melhores práticas de resposta a incidentes, traçando os passos para a análise de ameaças cibernéticas nos aspectos técnico e organizacional. Este guia tem o objetivo de auxiliar as empresas no desenvolvimento eficiente de processos de resposta a incidentes.

Destinado a profissionais de segurança da informação em cargos técnicos e organizacionais, bem como a iniciantes sem experiência prévia em segurança cibernética, este guia funciona como uma introdução à resposta a incidentes. Observe que o guia não se aprofunda em questões regulatórias ou informações legais sobre estruturas de gestão de segurança. Ele deve ser usado como material complementar em conjunto com as diretrizes aplicáveis referentes a resposta e divulgação de violações específicas para a sua organização. Além disso, o papel do seguro de proteção digital deve ser ponderado separadamente, pois as apólices podem conter diretrizes que divergem das recomendações apresentadas neste guia de resposta a incidentes.

O preparo eficiente contra incidentes cibernéticos permite que as organizações trabalhem com procedimentos e protocolos bem estabelecidos para a reação, atribuição e contenção de riscos mais rápidas. O objetivo deste documento é oferecer um guia de processos de resposta a incidentes para desenvolver a fase de preparação do ciclo de vida da gestão de incidentes exercendo um impacto financeiro e operacional mínimo às organizações ao facilitar a rápida contenção de incidentes cibernéticos.

Encorajamos os profissionais de segurança a incorporar esses conceitos e métodos de investigação em seus planos e processos de resposta a incidentes conforme apropriado. O guia pode ser lido do começo ao fim ou por seções, ou o leitor pode ler os capítulos que lhe sejam mais relevantes. O documento não oferece um plano passo a passo para lidar com incidentes cibernéticos, contudo, seu objetivo é ajudar as equipes de segurança a se prepararem e estabelecerem seus próprios processos.

As fases da gestão de incidentes descritas neste guia se alinham à estrutura SANS de resposta a incidentes recomendada, que consiste em seis fases. Essa estrutura foi projetada para enfatizar cada fase do ciclo de vida da gestão de incidentes e ajudar os profissionais em segurança a se prepararem para responder a incidentes com eficiência. Entretanto, não temos a intenção de que este seja um playbook estratégico. Incidentes cibernéticos são dinâmicos e, ainda que as estruturas ofereçam o embasamento necessário para um julgamento profissional sob uma perspectiva mais abrangente, os profissionais de segurança e funcionários preocupados com a segurança são incisivos em tratar desses incidentes.

Preparação

A primeira fase do ciclo de resposta a incidentes é a fase de preparação. As atividades e os esforços aplicados durante o desenvolvimento dessa fase influenciam significativamente a eficiência e eficácia das fases subsequentes. Portanto, a fase de preparação é crucial, devendo ser revisada e atualizada regularmente. Os elementos da fase de preparação englobam aspectos não técnicos, como processos e procedimentos, e componentes técnicos, como proteção de sistema, coleta de telemetria e treinamento. Com o enfoque necessário de tempo e recursos dedicado à preparação, as organizações podem criar uma base sólida para uma estratégia de resposta a incidentes robusta e resiliente.

Processos e procedimentos

Processos e procedimentos bem documentados são essenciais para o funcionamento eficiente de uma equipe de resposta a incidentes. Ao descrever e distribuir essas diretrizes para um pessoal selecionado a participar do processo de tratamento de incidentes, você garante a integridade das informações e o alinhamento com os objetivos de todas as partes envolvidas. Processos e procedimentos claramente definidos ajudam a manter a consistência na abordagem da equipe, facilitar a comunicação e colaborar para uma resposta a incidentes cibernéticos ágil e coordenada.

Plano de tratamento de incidentes

Um plano de tratamento de incidentes de incidentes que estabelece procedimentos claros para gerenciar os incidentes e a segurança cibernética e oferece as diretrizes necessárias a todos os envolvidos no processo. Os elementos a seguir devem ser incorporados no plano de tratamento de incidentes para assegurar uma abordagem abrangente ao responder ao incidente:

- **Definir as partes envolvidas:** identifique os principais envolvidos e atribua-lhes funções no processo de tratamento de incidentes, como posições de chefia em incidentes, equipe de TI complementar, organização e liderança, e também aos parceiros externos, como provedores de serviços de TI, autoridades legais e fornecedores de resposta a incidentes.
- **Classificação de incidentes e níveis de severidade:** estabeleça critérios de classificação de incidentes com base em fatores como potencial de impacto, sistemas afetados e tipo de ameaça. Defina os níveis de severidade para priorizar e direcionar os trabalhos de resposta a incidentes.
- **Procedimentos de escalonamento:** trace procedimentos claros para o escalonamento de incidentes que vão além da capacidade ou autoridade do pessoal de resposta inicial, incluindo o envolvimento de altos níveis de chefia ou o engajamento de peritos externos quando necessário.
- **Comunicação:** garanta uma comunicação eficiente durante as crises seguindo um padrão de resposta a incidentes com modelos de comunicação predefinidos para funcionários, clientes e parceiros. Incorpore também práticas de recuperação de desastre e planos de continuidade de negócios para avaliar canais suplementares no caso de falhas de comunicação por e-mail, mensagem ou videoconferência.
- **Inventário de patrimônio:** mantenha seu inventário atualizado para poder rastrear e administrar todos os equipamentos e softwares na organização. Essa informação é essencial para determinar a disseminação, o impacto e a resposta à ameaça.
- **Cronograma de resposta a incidentes:** crie um cronograma para cada fase do processo de resposta ao incidente, estipulando prazos para os principais marcos para assegurar a resposta organizada e imediata.
- **Documentação e relatório de incidentes:** padronize um processo para documentar todos os aspectos de um incidente, incluindo as medidas tomadas, as decisões feitas e os resultados alcançados. Esse documento será essencial nas análises pós-incidente e nas questões de âmbito legal ou regulatório.
- **Revisões pós-ação e melhorias contínuas:** implemente um processo para realizar revisões pós-ação seguidas a um incidente e avaliar a eficiência da resposta e identificar áreas para melhorar. Use esses insights para atualizar e melhorar o plano de tratamento de incidentes.

Ao incorporar esses elementos ao seu plano de tratamento de incidentes, a sua organização estará mais bem equipada para administrar e responder a incidentes de segurança cibernética com eficácia.

Documentação legal

Durante a fase de preparação, as empresas devem tratar das responsabilidades legais pertinentes a divulgação, regulamentos de tratamento de incidentes e outros aspectos relevantes da segurança cibernética. As seções a seguir ilustram algumas considerações legais comumente abordadas, mas cada organização deve conduzir sua própria análise de requisitos regulatórios específicos ao seu setor e local de atuação. Identifique as pessoas responsáveis por relatórios e conformidades legais na empresa e inclua essas pessoas no seu plano de resposta a incidentes com funções claramente definidas.

- **Responsabilidades de divulgação legais e regulatórias:** algumas organizações têm o dever legal ou são fomentadas a divulgar incidentes de acordo com o setor ou sua posição no mercado.
  - Organizações de setores de infraestrutura crítica
  - Agências governamentais
  - Empresas de capital aberto
- **Privacidade de dados:** siga à leis de proteção de dados que determinam as posturas de divulgação e confiabilidade para as agências incumbidas de manipular informações e para os clientes afetados ou pessoas cujos direitos de dados tenham sido comprometidos.
- **Retenção e destruição de dados:** estabeleça políticas e procedimentos de retenção, armazenamento e destruição segura dos dados coletados durante as atividades de resposta a incidentes de acordo com as leis e regulamentações aplicáveis.
- **Acordos e contratos com terceiros:** leia os acordos e contratos firmados com fornecedores, revendedores e parceiros para conhecer as obrigações de resposta a incidentes e os requisitos de notificação que os rege na eventualidade de uma violação ou um incidente.
- **Proteção de propriedade intelectual (PI):** analise os aspectos legais da propriedade intelectual da sua organização, incluindo segredos comerciais, patentes, direitos autoriais e marcas registradas, durante e após um incidente cibernético.
- **Relatório e transferência de dados entre fronteiras:** se a sua organização tem atuação internacional, pondere as implicações legais e os requisitos de transferência de dados e relatórios entre as diferentes jurisdições.
- **Direitos e deveres dos funcionários:** descreva os direitos e deveres legais dos funcionários no que tange aos incidentes de segurança cibernética, incluindo a obrigação de informar sobre incidentes e proteger informações confidenciais.
- **Documentação da apólice de seguro:** entenda o processo e os requisitos para abrir um sinistro com a seguradora.
  - Leia os termos e condições da apólice para determinar as inclusões e exclusões.
  - Consulte o seu departamento jurídico interno para assegurar o correto entendimento da cobertura.

Playbooks de resposta a incidentes

Os playbooks de resposta a incidentes oferecem diretrizes detalhadas passo a passo das ações a serem tomadas quando são identificadas ameaças específicas. Esses playbooks devem ser desenvolvidos tendo em mente riscos específicos e considerando-se a probabilidade e o potencial de impacto de diferentes cenários de ataque. Os elementos a seguir devem ser levados em conta quando estiver desenvolvendo os seus playbooks de resposta a incidentes:

- **Adaptados à sua organização:** assegure que seus playbooks sejam adaptados ao ambiente, características e recursos únicos da sua organização. Isso inclui o porte da empresa, o setor e os riscos específicos que a sua organização enfrenta.
- **Cenários e ameaças específicas:** recomendamos que as organizações mais sólidas desenvolvam playbooks para ameaças específicas, como determinados tipos de malware ou ameaças direcionadas. Contudo, para as organizações com recursos limitados, os playbooks devem abranger e cobrir ameaças variadas para serem aplicados em diferentes cenários.
- **Instruções claras e concisas:** os playbooks fornecerão instruções claras e concisas de cada etapa no processo de resposta. Isso ajuda as equipes de resposta a entender e executar com rapidez as ações necessárias durante um incidente.
- **Funções e responsabilidades:** defina com clareza as funções e responsabilidades de cada membro da equipe envolvido no processo de resposta. Isso assegura que cada pessoa saiba exatamente o que é esperado dela e possa contribuir de modo eficiente.
- **Comunicação e escalonamento:** inclua diretrizes para comunicação e escalonamento durante um incidente, por exemplo, ao notificar a gerencia ou solicitar apoio externo.
- **Integração com o plano de tratamento de incidentes:** assegure que seus playbooks estejam alinhados com o seu plano geral de tratamento de incidentes e ofereçam o apoio devido. Isso ajuda a manter consistência e coerência entre todos os esforços empenhados a responder ao incidente.

- Revisões e atualizações regulares: os playbooks devem ser revisados e atualizados regularmente para garantir que se mantenham relevantes e acompanhem a evolução das ameaças e as mudanças nas circunstâncias organizacionais.

Ao incorporar esses elementos ao seus playbooks de resposta a incidentes, a sua organização estará mais bem preparada para responder eficientemente a uma variedade de incidentes de segurança cibernética e minimizar os possíveis impactos.

Backups

Os backups são essenciais para assegurar a continuidade dos negócios e minimizar o impacto da perda de dados devida a acidentes, falhas no sistema ou ataques cibernéticos. Implementar uma estratégia de backup robusta envolve criar e validar backups regularmente, além de escolher uma variedade de opções de armazenamento para maximizar a disponibilidade de dados. Os elementos a seguir devem ser levados em conta quando estiver desenvolvendo sua estratégia de backup:

- **Frequência de backup:** determine a frequência apropriada para a criação de backups com base na criticalidade dos dados e no nível de risco admissível. Backups regulares ajudam a minimizar o potencial de impacto da perda de dados.
- **Tipos de backup:** utilize uma combinação de backups totais, incrementais e diferenciais para otimizar o espaço de armazenamento e facilitar a restauração eficiente dos dados.
- **Opções de armazenamento:** escolha diversas opções de armazenamento, incluindo backups locais, na nuvem e offline. Isso ajuda a garantir a disponibilidade dos dados e mitigar os riscos da perda de dados causados pelo armazenamento em um único local.
- **Priorização de dados críticos aos negócios:** focar na realização de backups de dados e sistemas essenciais aos negócios que são indispensáveis para a manter as operações básicas e dar apoio aos principais processos de negócios.
- **Criptografia do backup:** criptografe os backups para proteger dados confidenciais e prevenir o acesso não autorizado durante o armazenamento e a transmissão.
- **Validação do backup:** regularmente, avalie e valide os seus backups para garantir que sejam confiáveis e possam ser restaurados se necessários. Isso vai abranger testar o processo de restauração e verificar a integridade dos dados de backup.
- **Política de retenção:** implemente políticas de retenção de dados para gerenciar o armazenamento e descarte de backups de acordo com os requisitos legais, regulatórios e comerciais.
- **Plano de recuperação de desastres:** integre sua estratégia de backup ao seu plano geral de recuperação de desastre para garantir uma resposta eficiente e coordenada em eventos que haja a perda de dados.

Ao incorporar esses elementos à sua estratégia de backup, a sua organização estará mais bem preparada para se restabelecer.

Proteção de sistemas e redes

A proteção de sistemas e redes envolve reduzir a superfície de ataque minimizando as funcionalidades desnecessárias, o acesso aos sistemas e as conexões de rede. Ao implementar práticas eficazes de proteção, a sua organização pode diminuir a probabilidade de um ataque de sucesso. Considere os seguintes aspectos quando desenvolver a sua estratégia de proteção de sistemas e redes:

Patches

- **Programa de gerenciamento de patches:** estabeleça um programa para garantir a instalação de patches com consistência e prontidão na sua rede, equilibrando o uso de ferramentas automatizadas e semiautomatizadas.
- **Documentação:** mantenha um registro dos patches aplicados e das remoções necessárias.
- **Priorização:** priorize os patches com base em uma análise de riscos, priorizando o tratamento das vulnerabilidades com o potencial mais alto de impacto à sua organização.

Configuração

- **Auditoria de conformidade de segurança:** realize auditorias internas e externas contínuas para verificar a configuração e os parâmetros das ferramentas de segurança, identificando e solucionando possíveis problemas de configuração ou exclusões.
- **Controle de aplicativos:** implemente listas de bloqueio e permissão de aplicativos para limitar o número de aplicativos e as versões que podem ser executadas nos hosts, reduzindo o risco de softwares vulneráveis ou não autorizados serem explorados.
- **Controle de acesso à rede:** configure ferramentas de rede para restringir o acesso a IPs e portas apenas aos hosts internos e externos, minimizando o potencial de acesso não autorizado e a exfiltração de dados.

- **Princípio do privilégio mínimo:** garanta que os usuários na sua organização tenham direitos de acesso limitados a um mínimo necessário para desempenharem seus trabalhos, reduzindo o potencial de acesso não autorizado e o comprometimento dos dados.

Segurança da rede

- **Segmentação de rede:** divida sua rede em segmentos menores e separados para limitar o potencial de impacto de uma violação na segurança e dificultar que os hackers se movam lateralmente pela sua rede.
- **Configuração do firewall:** configure os firewalls para bloquear toda a entrada e saída de tráfego desnecessária e examine e atualize regularmente as regras para manter uma boa postura de segurança.
- **Sistemas de detecção e prevenção de invasão (IDPS):** implante um sistema IDPS para monitorar o tráfego da rede em busca de sinais de atividades maliciosas e tomar as devidas providências.

Monitoramento e telemetria

O monitoramento e a telemetria são componentes cruciais de uma estratégia eficiente de resposta a incidentes, pois oferecem insights valiosos do ambiente de uma organização e permitem a detecção antecipada de possíveis ameaças. Ao entender o seu ambiente e implementar as camadas apropriadas de detecção e defesa, você pode aumentar a eficácia e a capacidade da sua organização responder a incidentes.

Seu ambiente

Entender o seu ambiente é a base para um monitoramento e telemetria eficientes. Isso inclui:

- Inventário de patrimônio: mantenha registros atualizados de seus endpoints, servidores e a cobertura que recebem das suas plataformas de segurança relevantes.
- Topologia de rede: trace um diagrama claro da sua rede, incluindo pontos de entrada e saída, segmentação e pontos de controle, preferivelmente com todos os atualizados.

Camadas de detecção e defesa

Estabelecer várias camadas de detecção e defesa é essencial para ter uma estratégia de segurança abrangente. Considere as seguintes fontes de telemetria e assegure data e hora consistentes entre todas as fontes, usando UTC como o padrão recomendado:

- **Dispositivos de perímetro:** firewalls, sistemas IPS de prevenção de invasão, sistemas IDS de detecção de invasão, VPNs e proxies.
- **Proteção de endpoint:** Antivírus (AV), Antivírus Next-Gen (NGAV), Endpoint/Extended Detection and Response (E/XDR).
- **Log centralizado:** ferramentas SIEM para gerenciamento de informações e eventos de segurança, servidores syslog e armazenamento de dados na nuvem.
- **Autenticação:** serviços de autenticação multifator e IAM (Identity and Access Management).
- **Inteligência de ameaças:** inteligência tática para correlacionar e monitorar marcas para alertar sobre exposições externas.

Ferramentas e técnicas de monitoramento

Implementar as ferramentas e técnicas de monitoramento corretas é vital para se alcançar eficiência na resposta e identificação de incidentes. Considere as abordagens a seguir:

- **Monitoramento contínuo:** implante uma combinação de monitoramento periódico e em tempo real para manter uma visão ampla do seu ambiente.
- **Detecção de anomalia:** trabalhe com análises avançadas e algoritmos de machine learning para identificar padrões incomuns ou comportamentos que indiquem uma possível ameaça.
- **Correlação de log:** agregue e correlacione os dados de log de várias fontes para identificar padrões e tendências que possam ser um indicativo de ataque.
- **Priorização de alertas:** desenvolva um processo para priorizar alertas baseado em fatores como criticalidade, impacto potencial e nível de ameaça.

Mantendo o enfoque no seu ambiente, estabelecendo camadas robustas de deteção e defesa, e implementando ferramentas e técnicas de monitoramento eficientes você pode aumentar a eficácia e a capacidade da sua organização responder a incidentes de segurança com prontidão.

Comunicação

Uma comunicação eficiente é essencial durante a resposta a um incidente, pois permite coordenação e colaboração entre todos os envolvidos no processo. Essa seção descreve as considerações internas e externas sobre a comunicação dentro desse contexto, levando em consideração os aspectos legais.

Comunicação interna

- **Plano de comunicação:** estabeleça um plano de comunicação abrangente que detalhe os caminhos de escalonamento, os canais de comunicação e os principais pontos de contato. Esse plano deve ser revisado e atualizado periodicamente para garantir sua eficácia durante um incidente.
- **Equipe de resposta a incidentes:** forme uma equipe IRT de resposta a incidentes e nomeie um líder responsável por coordenar os trâmites de resposta. Confirme que os membros da equipe entendam suas funções e responsabilidades e mantenham uma linha de comunicação aberta durante todo o trabalho no incidente.
- **Canais seguros:** utilize canais seguros e confiáveis de comunicação para evitar o acesso não autorizado a informações confidenciais. Considere implementar aplicativos de mensagens criptografadas, e-mail seguro ou plataformas de comunicação dedicadas.
- **Modelos de resposta:** crie modelos predefinidos de resposta a incidentes para diferentes cenários, permitindo uma comunicação mais rápida e consistente. Esses modelos devem ser facilmente acessíveis, personalizáveis e alinhados com as diretrizes de comunicação da organização.
- **Atualização das partes envolvidas:** forneça atualizações regulares a todos os envolvidos no processo de gestão de incidentes, incluindo relatórios situacionais, medidas tomadas e resultados esperados. Mantenha a transparência para fomentar a segurança e a confiança no modo de tratamento de incidentes pela organização.

Comunicação externa

- **Estratégia de notificação:** desenvolva uma estratégia de notificação para clientes, fornecedores, parceiros e autoridades legais na eventualidade de uma violação de segurança ou outros incidentes que possam afetá-los. Essa estratégia deve descrever os critérios para notificação, canais apropriados e responsáveis designados pela comunicação.
- **Conformidade legal e regulatória:** assegure que as comunicações externas estejam conforme os requisitos legais e regulatórios, incluindo leis de proteção de dados, diretrizes de divulgação de responsabilidades e regulamentações específicas do setor. Consulte-se com um representante legal para confirmar que as comunicações estejam de acordo com todas as obrigações relevantes.
- **Pessoa de contato designada:** nomeie uma pessoa de contato ou uma equipe de relações públicas para lidar com questões de mídia e declarações públicas e garantir que a mensagem seja passada de modo consistente e preciso. essa pessoa ou equipe deve ser treinada em comunicação especializada em gestão de crises e relacionamento com a imprensa.
- **Preparação para comunicações externas:** prepare modelos de comunicação para vários cenários de incidentes para agilizar as notificações com pessoas de fora. Adapte esses modelos para que tratem das necessidades específicas das diferentes partes envolvidas, como clientes, parceiros e autoridades reguladoras.
- **Colaboração com outros departamentos:** Trabalhe de modo colaborativo com os departamentos jurídico, de relações públicas e outros departamentos relevantes para garantir que as comunicações externas estejam conforme os regulamentos, protejam a reputação da organização e mantenham a transparência com as partes afetadas.

Implementando essas estratégias de comunicação, a sua organização pode assegurar uma resposta coordenada e eficiente aos incidentes de segurança cibernética, mantendo a confiança e crença na sua organização e no modo como ela trata tais eventos.

Treinamento e conscientização em segurança

Instruir e educar seus funcionários sobre ameaças de segurança cibernética e melhores práticas é fundamental na postura de segurança geral de uma organização. Nessa seção, falaremos sobre os principais componentes de um programa abrangente de treinamento e conscientização em segurança, incluindo iniciativas de conscientização em segurança, conteúdo e frequência do treinamento, e exercícios e simulação de incidentes.

Programas de conscientização em segurança

- **Objetivos do programa:** estabeleça objetivos claros para o seu programa de conscientização em segurança, focando no conhecimento e nos comportamentos que os funcionários precisam adotar para proteger o patrimônio da organização e suas informações.
- **Treinamento desejado:** desenvolva materiais de treinamento adaptados para as diferentes funções e departamentos na organização, levando em conta suas responsabilidades únicas e seu acesso a informações confidenciais.

- **Atualizações constantes:** atualize regularmente o seu programa de conscientização em segurança para refletir a evolução do panorama de ameaças, incorporando as novas tendências de ataque e melhores práticas.
- **Métricas e avaliação:** rastreie e meça a eficiência do programa de conscientização em segurança usando indicadores KPI de desempenho, como engajamento dos funcionários, índices de conclusão de treinamentos e melhorias nos comportamentos em segurança.

Conteúdo e frequência de treinamento

- **Desenvolvimento de conteúdo:** crie um conteúdo de treinamento atraente e informativo que abranja uma totalidade de temas, como gerenciamento de senhas, conscientização sobre phishing, engenharia social e como navegar com segurança na internet.
- **Método de treinamento:** ofereça o treinamento em diversos formatos, incluindo cursos online, workshops presenciais e webinars interativos, para atender às diferentes preferências de aprendizado e disponibilidade individual.
- **Frequência:** programe sessões de treinamento regulares durante o ano todo, com uma frequência mínima recomendada trimestral. Ofereça também sessões de treinamento extraordinárias em resposta a incidentes específicos ou ameaças emergentes.
- **Aprendizado contínuo:** promova uma cultura de aprendizado contínuo oferecendo a seus funcionários o acesso a recursos adicionais, como artigos sobre o tema, vídeos e podcasts, que possam ajudar a expandir seus conhecimentos em segurança cibernética.

Exercícios e simulação de incidentes

- **Cenários realistas:** crie exercícios e incidentes simulados com base em cenários realistas que os funcionários possam enfrentar no seu dia a dia no trabalho. Esses cenários podem ajudar os funcionários a entender melhor o potencial de impacto de uma violação de segurança e a praticar suas habilidades de resposta.
- **Colaboração multifuncional:** envolva vários departamentos nas simulações, incentivando a colaboração e a comunicação entre as equipes de diferentes áreas de expertise.
- **Avaliação e feedback:** realize uma avaliação do desempenho dos funcionários durante os exercícios e incidentes simulados, passando a eles um feedback construtivo e identificando áreas que podem ser melhoradas.
- **Lições aprendidas:** compartilhe as lições aprendidas e os ensinamentos adquiridos com os exercícios simulados com toda a organização, reiterando os conceitos básicos e as melhores práticas.

Ao implementar um programa de treinamento e conscientização em segurança, as organizações podem empoderar os funcionários com conhecimentos e habilidades necessários para identificar e responder às ameaças de segurança cibernética, restringindo o risco de ataques bem-sucedidos.

Equipe de resposta a incidentes

Uma equipe eficiente é essencial para assegurar uma resposta a incidentes de segurança cibernética coordenada e imediata. Nesta seção, trataremos de funções e responsabilidades, composição da equipe e da importância do apoio e expertise externos em resposta a um incidente.

Funções e responsabilidades

- **Gerente de resposta a incidentes:** supervisiona o processo de resposta a incidentes, coordena as atividades da equipe e assegura uma comunicação eficiente entre os membros da equipe e com os colaboradores externos.
- **Analistas de segurança:** investigam e analisam os incidentes de segurança, oferecendo expertise técnica na identificação da causa primária, escopo e impacto do incidente.
- **Analistas forenses:** realizam tarefas forenses digitais, incluindo coleta, análise e preservação de provas para apoiar as investigações e processos legais.
- **Operações de TI:** auxiliam nos esforços de contenção, erradicação e recuperação, gerenciando a infraestrutura do sistema e implementando as mudanças necessárias para prevenir futuros incidentes.
- **Jurídico e regulatório:** fornecem diretrizes sobre requisitos legais e regulatórios relacionados à resposta a incidentes, garantindo a correta divulgação e relatórios.
- **Comunicações e relações públicas:** gerenciam as comunicações internas e externas, transmitindo as mensagens apropriadas para as partes afetadas, como funcionários, clientes, parceiros e autoridades reguladoras.

Composição da equipe de resposta a incidentes

- **Representação multifuncional:** forme uma equipe diversificada que represente vários departamentos, incluindo TI, segurança, jurídico, RH e comunicações, para cobrir a natureza multidisciplinar da resposta a incidentes.
- **Competências e expertise:** assegure-se de que os membros da equipe tenham domínio nas competências e expertise necessária para desempenhar suas funções designadas, providenciando a todos oportunidades contínuas de treinamento e desenvolvimento.
- **Disponibilidade e rodízio:** estabeleça uma equipe que esteja disponível 24 horas por dia, sete dias por semana, usando um sistema de plantão com rodízio de chamadas ou turnos dedicados para manter uma cobertura ininterrupta.

Expertise e apoio externo

- **Fornecedores terceiros:** envolva peritos externos, como consultores em segurança cibernética ou provedores de serviços de segurança gerenciada (MSSP), para complementar sua capacidade interna e oferecer conhecimento especializado em áreas como crimes digitais ou inteligência de ameaças.
- **Conselho jurídico:** contrate um conselho jurídico externo com expertise em leis de segurança cibernética e privacidade de dados para esclarecer sobre os requisitos de conformidade e divulgação, e também para representar a organização em litígios e processos relacionados a incidentes de segurança.
- **Autoridades legais e agências reguladoras:** estabeleça relacionamentos com agências reguladoras, entidades e autoridades legais relevantes para facilitar a cooperação e compartilhar informações durante as investigações de um incidente.
- **Colaboração do setor:** participe de fóruns de segurança cibernética específicos do setor e grupos de compartilhamento de informações para exercer a troca de inteligência de ameaças e melhores práticas com outras organizações para se manter a par das ameaças emergentes e novas tendências.

Ao formar uma equipe de resposta a incidentes bem estruturada e complementá-la com apoio e expertise externos, as organizações podem gerenciar melhor os incidentes de segurança cibernética e minimizar seu potencial de impacto.

Identificação

A fase de identificação é crucial para detectar a presença de um invasor em uma rede ou sistema. O monitoramento contínuo da telemetria da rede é essencial para minimizar o tempo entre a invasão e a identificação. Quanto mais rápido a equipe reagir, menor será o impacto em confidencialidade, integridade e disponibilidade de dados, sistemas e redes. As soluções MDR oferecem um apoio valioso ao processo ao proporcionar as funcionalidades de detecção e resposta a ameaças gerenciadas por peritos.

Principais componentes de identificação

- **Telemetria de dispositivos e rede:** o monitoramento que abranja várias das possíveis fontes de ameaças, como mencionado na seção de Telemetria, é essencial para a detecção e resposta em tempo real. Implementar uma solução MDR pode aprimorar esse processo.
- **Notificações externas:** colaborar com as autoridades legais e outras fontes externas para reunir e analisar a inteligência de ameaças permite a identificação mais rápida de possíveis invasões.
- **Inteligência de ameaças:** monitorar a dark web e sites clandestinos para identificar empresas expostas a possíveis comprometimentos para venda posterior melhora as capacidades de detecção.
- **Informe de usuários:** incentive os usuários para que informem sobre e-mails ou links suspeitos e respondam rapidamente a essas possíveis ameaças para garantir que esses contextos sejam direcionados ao pessoal que lida com incidentes.

Processos sólidos devem ser estabelecidos para categorizar o grau de severidade de um incidente com base nos seguintes critérios:

- **Fidelidade:** verifique a confiabilidade da fonte (por ex., IPS, FW, AV, XDR).
- **Criticalidade:** considere a importância do sistema afetado.
- **Má intenção:** avalie o comportamento suspeito, que pode fornecer pistas que levam a descobrir uma violação ainda desconhecida.
- **Tipo de incidente:** use estruturas como Cyber Kill Chain e MITRE ATT&CK para classificar os incidentes.
- **Data/hora:** assegure consistência em registros de data/hora usando UTC, NTP e outros padrões comuns para normalizar os dados.

Tipos de incidentes

A NIST define duas categorias de incidentes:

- **Precursor:** detecta sinais de reconhecimento, como atividade de varredura destinada a identificar portas abertas e vulnerabilidades de software. Soluções MDR podem ser particularmente úteis nesse contexto. Identifique explorações conhecidas de vulnerabilidades de código remoto presentes na infraestrutura das organizações.
- **Indicador:** identifique incidentes com vários tipos de indicadores, como alertas de malware, mudanças em arquivos ou no Active Directory, ou comportamentos singulares de usuários, como logins via RDP em horários incomuns, e inicie a resposta apropriada ao incidente. O MDR pode oferecer suporte adicional na detecção e resposta a tais incidentes.

Ao implementar uma estratégia de monitoramento abrangente, aproveitar as notificações externas e a inteligência de ameaças, incentivar o uso de relatórios e utilizar critérios bem definidos de categorização de incidentes, as organizações podem aprimorar sua postura geral de segurança. Além disso, as soluções MDR podem oferecer suporte adicional na detecção e resposta a incidentes com eficiência. Uma fase de identificação robusta não apenas reduz o impacto dos incidentes de segurança, mas também fomenta uma cultura de segurança proativa na organização, promovendo a continuidade dos negócios e protegendo seus bens valiosos.

Arquivos, diretórios, processos e persistência potencialmente suspeitos

Entender e identificar arquivos, diretórios, processos e mecanismos de persistência pode ajudar na detecção antecipada de incidentes.

- **Arquivos e diretórios:** arquivos e diretórios incomuns e inesperados podem indicar um incidente de segurança. Exemplos:
  - Arquivos com nomes ou extensões pouco convencionais
  - Arquivos em locais não esperados
  - Diretórios contendo dados confidenciais que não deveriam estar acessíveis
- **Processamentos:** Processamentos suspeitos podem ser um sinal de atividades maliciosas em um sistema. Exemplos:

- Processamentos com alto uso de CPU ou memória
- Processamentos executados de locais não esperados
- Processamentos que tentam acessar recursos ou dados confidenciais

- **Persistência:** os invasores costumam estabelecer mecanismos de persistência para manter o acesso aos sistemas comprometidos. Exemplos de técnicas de persistência:
  - Tarefas agendadas ou operações cron que executam scripts maliciosos
  - Malware que se reinstala a cada remoção ou reinicialização
  - Chaves de registro ou itens de reinicialização que lançam processos maliciosos
- **Acesso a credenciais:** acesso não autorizado a credenciais pode levar a comprometimentos futuros de sistemas e dados confidenciais. Exemplos:
  - Ataques de força bruta a contas de usuários
  - Campanhas de phishing direcionadas a credenciais de funcionários
  - Despejo de credenciais de sistemas comprometidos
- **Acesso e bases operacionais adicionais:** os invasores podem tentar estabelecer uma base de operações dentro do ambiente da organização para expandir seu acesso e controle. Exemplos:
  - Contas comprometidas de usuários com privilégios elevados
  - Exploração de vulnerabilidades sem patches em sistemas ou aplicativos
  - Movimentos laterais internos na rede para acessar recursos adicionais

Ao reconhecer esses tipos de incidentes e seus exemplos, as organizações podem identificar com maior eficiência as possíveis ameaças e responder de acordo. Conscientizar-se sobre esses vários tipos de incidentes é essencial para a capacidade de uma organização detectar e mitigar incidentes de segurança com prontidão.

Análise forense

A análise forense é um aspecto crucial no processo de resposta a incidentes, pois ajuda as organizações a identificar a causa primária de um incidente, entender o seu impacto e coletar provas para apoiar as investigações ou processos legais. A seguir estão alguns dos principais elementos de uma análise forense:

Ferramentas e técnicas forenses

Há várias ferramentas e técnicas forenses disponíveis para auxiliar na análise de sistemas e redes durante uma resposta a incidentes. Essas ferramentas podem ajudar na coleta, análise e preservação de dados. Exemplos de ferramentas e técnicas forenses:

- Ferramentas de clonagem e geração de imagem de disco para preservar o estado de um sistema comprometido
- Ferramentas de análise de memória para investigar dados voláteis e identificar processos maliciosos
- Ferramentas de análise de tráfego de rede para examinar a atividade da rede e identificar possíveis indicadores de comprometimento
- Ferramentas de análise de logs para revisão dos logs de sistema e aplicativos em busca de atividades suspeitas

Coleta e preservação de provas

A coleta e preservação adequadas das provas são essenciais na análise forense para garantir a integridade dos dados e manter sua admissibilidade em processos legais. Algumas das melhores práticas de coleta e conservação de provas incluem:

- Documentação de cada passo do processo de coleta de provas, incluindo as ferramentas e técnicas usadas.
- Criação de um cronograma de eventos minucioso do incidente.
- Uso de bloqueadores de gravação e outras ferramentas forenses para prevenir a alteração das provas durante a coleta.
- Proteção dos dados coletados em contêineres com mecanismos contra adulteração ou meios de armazenamento criptografado.
- Garantia de que os dados coletados sejam armazenados em um ambiente protegido e controlado.

Cadeia de custódia

Manter a custódia devida é essencial para conservar a integridade das provas e assegurar sua admissibilidade em processos legais. Uma cadeia de custódia refere-se à documentação e ao rastreio da manipulação, armazenamento e transferência de provas durante a investigação. Para manter uma cadeia de custódia corretamente, as organizações devem:

- Registrar os detalhes de cada pessoa que manipulou as provas, incluindo nome, função e informações de contato.
- Documentar a data, hora e localização de cada transferência ou manipulação das provas.
- Manter um registro de todas as ações que foram realizadas com as provas, como cópia, análise ou armazenamento.
- Garantir que as provas sejam sempre armazenadas e transportadas com segurança, usando selos e fitas antifraude ou armazenamento criptografado quando necessário.

Ao incorporar análises forenses ao processo de resposta a incidentes, as organizações têm em mãos insights valiosos sobre a natureza e o escopo dos incidentes de segurança, coletam provas cruciais e oferecem apoio extra às investigações ou processos legais. Entender e implementar ferramentas, técnicas e práticas forenses apropriadas é essencial para conduzir uma análise plena e eficaz.

Exfiltração de dados

A exfiltração de dados refere-se à transferência não autorizada de informações ou dados confidenciais de sistemas ou redes de uma organização para um local externo, normalmente controlado por um invasor. Detectar e prevenir a exfiltração de dados é crucial para minimizar o impacto de uma violação à segurança e proteger bens valiosos. Para tratar de modo eficaz da exfiltração de dados, as organizações devem considerar os seguintes aspectos:

- **Monitoramento e alerta:** implementar um sistema de monitoramento abrangente que detecte transferências de dados ou padrões de tráfego de rede incomuns, como transferência de grandes arquivos, comunicação com endereços IP suspeitos ou várias tentativas de login com falha. Assegure que sejam postos em prática mecanismos de alerta adequados para notificar as equipes apropriadas sobre possíveis incidentes de exfiltração de dados.
- **Soluções DLP de prevenção contra a perda de dados:** implantar soluções DLP para identificar e prevenir que dados confidenciais sejam transferidos para fora da rede da organização. As soluções DLP podem ajudar a identificar e bloquear a transferência não autorizada de informações confidenciais com base em políticas e regras predefinidas.
- **Criptografia:** criptografar dados confidenciais em repouso e em trânsito para diminuir o valor dos dados para o invasor no caso de uma tentativa de exfiltração de sucesso.
- **Conscientização e treinamento do funcionário:** educar e instruir os funcionários sobre os riscos da exfiltração de dados e a importância de seguir as políticas de segurança, como não compartilhar informações confidenciais através de canais sem segurança ou com pessoas não autorizadas.

Validação e priorização

Uma vez que um possível incidente de segurança seja identificado, é essencial validar o incidente e priorizar a resposta com base na severidade e possível impacto na organização. A validação e priorização envolvem as seguintes etapas:

- **Validação do incidente:** confirmar que o incidente é um evento de segurança genuíno e não um falso positivo. Isso é possível analisando os dados disponíveis, correlacionando esses dados com uma inteligência de ameaças conhecidas e revisando o contexto do evento.
- **Priorização do incidente:** avaliar o potencial de impacto do incidente nos bens, operações e reputação da organização. Considerar fatores como o tipo dos dados ou sistemas envolvidos, a extensão do comprometimento e as possíveis consequências do incidente.
- **Níveis de segurança:** atribuir um nível de severidade ao incidente com base na avaliação de priorização. Os níveis de severidade podem ser definidos usando uma escala predefinida, como baixa, média, alta ou crítica, e então usados para direcionar a equipe de resposta a incidentes na determinação dos recursos apropriados e urgência de ação.
- **Plano de resposta:** de acordo com o nível de severidade e a natureza do incidente, selecione o plano de resposta apropriado no playbook de resposta a incidentes da organização. Esse plano deve descrever os passos necessários para conter, investigar e remediar o incidente, bem como os procedimentos de comunicação e relatório exigidos.

Ao identificar, validar e priorizar os incidentes de segurança com eficiência, as organizações podem assegurar que seus recursos também sejam alocados com eficiência e seus esforços de resposta sejam direcionados aos incidentes mais críticos, minimizando o impacto geral na organização.

Contenção

O objetivo principal da contenção é minimizar danos maiores, isolando sistemas que foram identificados como comprometidos ou que levantaram suspeitas de estar comprometidos. Essa etapa ajuda a evitar a difusão de incidentes, como a propagação de malwares ou exfiltração continuada de dados, e facilita a preservação de um sistema em um estado em que indícios adicionais possam ser coletados. Estratégias de contenção adequadas podem se mostrar valiosas para a investigação, como a coleta a Indicadores de Comprometimento (IOCs) que serão documentados e utilizados em análises futuras.

Contenção de curto prazo

Ações de contenção de curto prazo com medidas imediatas para limitar o impacto do incidente. Normalmente, elas são realizadas ao identificar o computador comprometido para atender ao objetivo principal de conter a ameaça em andamento. Exemplos de medidas de contenção de curto prazo:

- **Isolamento com base no host:** use recursos de plataformas de segurança para isolar hosts comprometidos, como o Sophos Intercept X Advanced, enquanto mantém uma conexão ativa para investigação posterior.
- **Bloqueio de hashes SHA256:** utilize o Sophos Intercept X Advanced para bloquear arquivos maliciosos pelo hash SHA256, evitando a sua execução.
- **Rede isolada:** altere as políticas de roteamento do switch, roteador ou firewall para impedir que o segmento da rede que contém o computador identificado se comunique com outros computadores e dissemine a ameaça.
- **Isolamento manual:** desconecte o cabo ethernet da rede ou desative a placa de rede (Wi-Fi) do computador em resposta a um comprometimento identificado.
- **Redefinição de conta:** redefina todas as contas de usuário desconhecidas ou com suspeita de comprometimento.

Contenção de longo prazo

A contenção de longo prazo se concentra na prevenção da disseminação de um mesmo incidente para outros computadores na rede após as investigações iniciais serem concluídas. Exemplos de medidas de contenção de longo prazo:

- Bloqueio de conexões de rede a URLs suspeitas e servidores de comando e controle (C2) identificados durante a investigação.
- Suspensão de contas de domínio comprometidas, redefinição ou suspensão de senhas de domínios e contas administrativas locais, e execução de uma redefinição de senha que englobe todo o domínio se um incidente de grande escala não puder ser determinado.
- Implementação do isolamento automático de um dispositivo com base em um status mínimo de integridade do computador.
- Instalação de agentes de segurança em computadores sem proteção ou computadores que passaram por limpeza e apagamento para assegurar visibilidade e proteção.

Melhores práticas

Para assegurar uma contenção eficaz, considere estas práticas:

O que fazer

- Isole a máquina usando uma das opções acima.
- Documente os passos seguidos, registre a hora, a ação e quem realizou a ação.
- Considere seus planos de resposta a incidentes e estratégia de contenção, especialmente se estiver respondendo a um processo de litígio. Capture imagens criminalistas e pondere o envolvimento da seguradora de proteção digital.
- Categorize a ameaça de acordo com o seu nível de ataque e notifique a gerência se for um incidente de alta gravidade.
- Determine os IOCs para ajudar na investigação e reúna provas.
- Informe as partes envolvidas, como gerência, departamento jurídico e de relações públicas, sobre a gravidade do incidente e seu potencial de impacto.

- Monitore os sinais de retaliação ou escalonamento do invasor durante o processo de contenção, pois o invasor poderá tentar infligir mais danos quando se der conta de que suas atividades foram descobertas.
- Assegure-se de que as medidas de contenção sejam reversíveis, para o caso de serem constatados falsos positivos e consequências inesperadas.
- Realize uma análise completa do incidente para identificar as causas primárias e melhorar a sua postura de segurança e o seu processo de resposta a incidentes utilizando-se da experiência adquirida.

O que não fazer

- Desligue ou reinicialize o computador comprometido.
- Aja de maneira precipitada sem consultar o gerente responsável conforme definido no seu plano de resposta a incidentes.
- Instale backups imediatamente sem concluir a coleta de IOCs iniciais e as investigações.
- Torne o incidente público ou compartilhe informações confidenciais com pessoas não autorizadas, pois isso pode alertar o invasor e comprometer o processo de contenção.
- Trabalhe apenas com ferramentas ou processos automatizados para contenção; envolva a perícia e o julgamento humanos para a tomada de decisões ponderadas.
- Esqueça-se de considerar o possível impacto das ações de contenção nos negócios, como tempo de inatividade ou perda de funcionalidade, e ponderar esses fatores em comparação aos riscos de não realizar tais ações.
- Descuide do seu plano de resposta a incidentes e procedimentos, lembrando-se de atualizá-los com os ensinamentos adquiridos com o processo de contenção para se preparar melhor para futuros incidentes.

Lembre-se de que não existe uma abordagem única que cubra toda e qualquer situação e que as medidas tomadas devem considerar o tipo de incidente, o panorama de operação da rede e a acessibilidade a ela. Ainda que a contenção interrompa a ameaça imediatamente e dê tempo para você pensar nas próximas ações, esse não é exatamente o passo mais importante no tratamento de um incidente. As empresas devem se manter atentas ao risco constante a que estão expostas, sabendo que os invasores podem aumentar a intensidade do ataque cibernético quando se derem conta de que foram pegos.

Erradicação

A erradicação é o processo de eliminar totalmente uma ameaça ou invasor de um ambiente. Geralmente envolve vários estágios com o objetivo de identificar, documentar e erradicar todas as atividades dos agentes de ameaças, alterações ao sistema, malwares e execuções na rede e nos computadores. Como a maioria dos ataques cibernéticos de alto impacto se respaldam em várias bases de operações e na coordenação prática realizada pelas mãos dos hackers, é essencial identificar as irregularidades que as varreduras não detectam. Ao erradicar uma ameaça, é de extrema importância considerar todos os possíveis efeitos residuais.

Existem duas estratégias principais na erradicação: recompilar ou refazer a imagem dos computadores e aplicar uma remoção direcionada. As duas têm seus pontos fortes e pontos fracos e são geralmente realizadas em conjunto para oferecer o máximo de eficácia.

Recompilar ou refazer a imagem do computador

A forma mais eficiente de erradicar bens comprometidos é recompilar ou refazer a imagem dos hosts, assegurando a reversão completa para um estado descomprometido. Esse processo é mais simples se as organizações implantarem imagens de software padrão nos hosts e tiverem acesso a imagens mestre para a recuperação. A imagem mestre deve ser criada antes da implantação na produção para garantir que não haja comprometimentos prévios.

No caso de servidores críticos, como sistemas ERP, servidores de e-mail e servidores de arquivos, a restauração a partir de uma imagem mestre é incomum devido ao potencial de perda de dados e custos associados. Portanto, as organizações podem restaurar a partir de um arquivo de backup limpo (por exemplo, servidor de backup, fita, nuvem ou outras mídias). Esse processo exige verificar a disponibilidade e integridade dos arquivos de backup e escolher um estado de recuperação que não esteja infectado. Para assegurar a estratégia de recompilação ou recriação de imagem mais eficaz, as organizações devem investigar IOCs e TTPs (Táticas, Técnicas e Procedimentos) em toda a rede, com um enfoque especial nos computadores vulneráveis.

Remoção direcionada

A estratégia de remoção direcionada visa identificar todos os componentes de um malware e seus artefatos, desvendar as alterações mais significativas ao sistema realizadas pelo adversário e removê-las ou revertê-las ao seu estado pré-comprometimento. Essa abordagem é necessária em computadores que dão suporte a sistemas de produção, sistemas de controle industrial ou outras operações comerciais básicas em que a perda de dados ou um período de inatividade podem causar sérias consequências.

A remoção direcionada é geralmente implementada usando uma combinação de ferramentas e equipes de resposta especializadas que saem no encalço das ameaças com base em IOCs observados, inteligência de ameaças associada e experiências pessoais com TTPs adversários. As organizações podem usar a remoção direcionada para obter um entendimento mais aprofundado do ataque, extraindo ensinamentos para implementar melhorias a longo prazo e reduzir o risco de ataques cibernéticos futuros.

Por exemplo, se um invasor for bem-sucedido no comprometimento de um host baseando-se em vulnerabilidades existentes, configurações incorretas ou um comprometimento prévio dormente, a erradicação deverá incluir também a mitigação dessas deficiências para prevenir que o host se torne um vetor de reinfecção ou de um novo ataque. A análise da causa primária pode ajudar as organizações a entender os passos que um invasor seguiu até que o impacto foi notado e encontrar o marco zero para prevenir ataques futuros.

Recomenda-se que as empresas continuem a documentar suas descobertas e usem estruturas como a MITRE ATT&CK para conceitualizar a arquitetura de um ataque. Essa abordagem estruturada ajuda a identificar a causa primária de um incidente e permite que as organizações melhorem sua postura geral de segurança.

Recuperação

O objetivo da fase de recuperação é proceder seguindo uma abordagem em estágios para recolocar os computadores e os sistemas afetados da organização de volta à sua operação normal, restaurando sua funcionalidade plena como antes da violação. A estratégia de recuperação depende do incidente, pois determinados incidentes podem levar ao isolamento de alguns computadores com pequeno impacto operacional, enquanto os ataques maiores, como ransomwares, podem ter como alvo vários computadores, causando um impacto operacional significativo e inatividade comercial. Portanto, os planos de recuperação devem ser ajustados ao ataque.

- Um único host afetado por um e-mail de phishing com o conteúdo detectado e eliminado pelo agente de proteção do endpoint pode garantir o isolamento do computador sob a investigação e os cuidados de um analista de segurança com um mínimo de impacto operacional.
- A detecção antecipada de um botnet na rede que afete o computador de dois ou mais usuários com mecanismos de persistência pode levar ao isolamento e à recompilação imediata desses computadores, resultando em tempo de inatividade para os funcionários, porém em um impacto operacional mínimo para os negócios.
- Um ataque de ransomware que abranja toda a rede com um tempo médio de permanência de várias semanas e uma causa primária identificada levará ao isolamento de não apenas endpoints e servidores, mas também de e-mails, VPNs, contas do Active Directory e outros serviços. Nesse caso, as equipes de resposta a incidentes devem manter medidas de contenção em ação até que o ataque esteja sob controle por meio da identificação de bases operacionais, patches e computadores com imagens refeitas. As estratégias podem incluir criar uma rede "limpa" alternativa, reconstruindo a rede sem nenhum computador afetado e reintegrando os computadores um a um. A decisão de reintegrar os computadores isolados deve se basear em um nível suficientemente baixo de reentrada ou reinfecção, e as equipes de resposta devem informar esse risco à gerência para estabelecer um cronograma adequado de risco e abordagem.

Uma abordagem cuidadosa

A recuperação de computadores é uma tarefa que exige foco e atenção aos mínimos detalhes do sistema, pois o excesso de confiança sobre a erradicação de uma ameaça e a fatiga para exterminar o incidente podem prejudicar um bom julgamento. É essencial que se mantenha o controle e a atenção redobrada sobre:

- A integridade geral do sistema de um computador afetado que é reintegrado a uma rede, aplicando testes de integridade e estabilidade do sistema.
- A aplicação de patches às vulnerabilidades de segurança, especialmente após restaurar um computador de uma versão anterior que pode estar suscetível a um ataque repetido.
- A certeza de que controles e políticas de segurança adequados são aplicados a cada computador:
  - O agente de segurança deve ser implantado em todos os computadores reintegrados.
  - As exclusões de varredura devem ser mínimas, com exclusões e aplicações específicas personalizadas para os itens, computadores e grupos de usuários excluídos.
- As varreduras e buscas pela presença de IOCs identificados em ataques e bases operacionais que um agente de ameaça possa ter deixado para trás.

Além disso, as equipes de resposta a incidentes e os analistas de segurança devem continuar monitorando o ambiente por atividades de ameaças e pesquisando proativamente atividades comuns de vetores de ameaça para identificar antecipadamente as ameaças e responder conforme elas surgem.

A fase de recuperação não precisa seguir à fase de erradicação completa, podendo ser conduzida de modo intercambiável, pois os computadores restaurados a um estado de sistema íntegro podem ser reintegrados ao ambiente de produção.

Revisão pós-incidente e lições aprendidas

Após recuperar-se com sucesso de um incidente de segurança cibernética, é essencial que seja realizada uma revisão pós-incidente e que as lições aprendidas e seus ensinamentos sejam identificados. Esse processo ajudará a sua organização a analisar a eficiência da sua resposta ao incidente, identificar áreas de melhoria e implementar mudanças ao plano de resposta a incidentes. Ao fazer isso, você pode se preparar melhorar para incidentes futuros e minimizar o risco de violações semelhantes.

Revisão pós-incidente

Análise da eficiência da resposta a incidentes

Para avaliar a eficácia da resposta a incidentes da sua organização, reveja as medidas de ação realizadas pela resposta a incidentes e meça seus resultados. Considere os aspectos a seguir:

- Tempo necessário para detectar, conter e remediar o incidente
- Comunicação e coordenação entre membros da equipe e com parceiros externos (incluindo autoridades legais, fornecedores)
- A adequação da estratégia de contenção, erradicação e recuperação
- A precisão e utilidade das informações fornecidas pelas ferramentas de monitoramento e detecção

Identificando áreas de melhoria

Após analisar a eficiência da resposta ao incidente, identifique as áreas em que sua organização pode melhorar seus processos e procedimentos. Algumas áreas comuns de melhoria podem incluir:

- Programas de conscientização e treinamento de funcionários
- Capacidade de detecção e monitoramento de incidentes
- Atualizações do plano de resposta a incidentes
- Controles técnicos e medidas de segurança
- Funções e responsabilidades da equipe de resposta a incidentes
- Comunicação e colaboração com as partes externas

Implementando alterações e atualizações ao plano de resposta a incidentes

Após identificar áreas de melhoria, é essencial implementar mudanças ao plano de resposta a incidentes da sua organização. Certifique-se de:

- Atualizar o plano com novos procedimentos, diretrizes ou medições técnicas conforme necessário.
- Informar sobre as alterações a todas as partes relevantes, incluindo funcionários, gerência e colaboradores externos.
- Realizar exercícios e treinamentos regulares para assegurar que o plano de atualização seja entendido e possa ser executado com eficiência.
- Monitorar e avaliar a eficiência das alterações com o decorrer do tempo e fazer ajustes quando necessário.

Ao realizar uma revisão pós-incidente completa e identificar as lições aprendidas, a sua organização pode aprimorar a postura de segurança cibernética e se preparar melhorar para incidentes futuros. Lembre-se de que o processo de resposta a incidentes é um processo contínuo, e que revisar e atualizar regularmente o seu plano ajudará a organização a se manter resiliente diante da evolução das ameaças cibernéticas.

Lições aprendidas

As lições aprendidas dependerão do tipo de incidente e do processo de tratamento do incidente, e representam as áreas identificadas para melhorias. Essa fase de ensinamento e aprendizado é uma etapa crítica que muitas vezes é ignorada assim que passa o sufoco da situação de emergência, e o apoio executivo é retirado e todos voltam ao trabalho e retomam as operações rapidamente. Portanto, é ainda mais importante que a fase de lições aprendidas ocorra imediatamente após a fase de recuperação para prender a atenção dos executivos para que entendam os detalhes do incidente e acordem em melhorias para mitigar riscos futuros.

Uma ideia seria escrever uma reavaliação do incidente incluindo um resumo executivo que pudesse ser compartilhado por todos e entendido também pelo pessoal sem conhecimentos técnicos de dentro e de fora da empresa. Esse documento de reavaliação deve ser colaborativo, permitindo que vários envolvidos façam comentários e edições, e oferecer um consenso conclusivo na forma de um relatório final, incluindo os detalhes técnicos e as lições aprendidas.

Dada a amplitude do espectro das áreas passíveis de melhoria, algumas áreas comuns foram relacionadas abaixo, porém elas não são um registro rígido de possibilidades.

Melhores práticas de segurança recomendadas:

- Desative e remova softwares, aplicativos e equipamentos desatualizados do patrimônio corporativo para minimizar o risco de explorações.
- Estabeleça um processo robusto de gerenciamento de patches para software e hardware que se alinhe com as necessidades da organização e assegure a atualização de patches regularmente.
- Instale agentes de proteção de endpoint baseados na nuvem em todos os computadores do patrimônio corporativo para detectar e neutralizar ameaças maliciosas.
- Implemente a autenticação multifator (MFA) para VPN, RDP e outros serviços que exigem a autenticação para aprimorar a segurança.
- Defenda a infraestrutura implementando mecanismos de controle de segurança básicos e protegendo os serviços voltados à internet contra o acesso não autorizado.
- Reforce o gerenciamento de credenciais impondo requisitos de complexidade, usando gerenciadores de senhas e fazendo a rotatividade regular de credenciais.
- Implemente protocolos de autenticação de e-mail, como DMARC, DKIM e SPF, para se proteger contra e-mails de phishing e falsificações.

Configuração da rede:

- Implemente o controle de acesso de rede (NAC) para adicionar uma camada extra de segurança e defender-se contra dispositivos ilegítimos e ameaças maliciosas.
- Segregue as redes usando VLANs para proteger sistemas críticos e confidenciais e isolar plataformas e serviços voltados à internet na DMZ.

Fortalecimento:

- Implemente o bloqueio de GEO IP em firewalls para prevenir o tráfego de rede indesejado com base na origem geográfica.
- Implante soluções de controle de aplicativos como o AppLocker para impedir a instalação ou execução de aplicativos e arquivos não autorizados dentro do patrimônio corporativo.
- Fortaleça seus controladores de domínio revisando e removendo serviços desnecessários, softwares sem suporte e protocolos herdados que possam apresentar um risco à segurança.

Precauções de segurança e gerenciamento proativo:

- **Auditoria da infraestrutura:** Realize auditorias regulares da configuração das portas em toda a infraestrutura da organização voltada à internet, assegurando que apenas os serviços de protocolos necessários sejam permitidos e as portas de fluxo de rede estejam adequadamente configuradas.
  - Por exemplo, eth0 é voltada à internet e eth1 só é alcançada internamente.
- **Auditoria de controle da web:** revise as configurações de tráfego da web regularmente nos servidores proxy e plataformas de fluxo de tráfego da web semelhantes. Restrinja os controles de segurança onde for aplicável, seguindo o princípio do privilégio mínimo. Implemente uma política de bloqueio ou negação padrão. Por exemplo:
  - Bloqueie tipos de arquivo que impõem riscos desnecessários à sua organização.
  - Revise as políticas de categorização padrão de URLs e domínios não categorizados.
  - Exporte dados estatísticos para identificar anomalias, padrões ou eventos recorrentes suspeitos e maliciosos.
  - Assegure-se de que grupos e políticas sejam atualizados de acordo com o princípio RBAC de controle de acesso baseado em função.
- **Auditoria da conta:** realize auditorias regulares de contas de administrador local não aprovadas e não convencionais, ou semelhantes, dentro da organização com o intuito de remover tais contas.
- **Logs de eventos do Windows:** configure os logs de eventos do Windows para conservar os dados, como o aumento do tamanho dos logs de eventos do Windows Core através de políticas de grupo ou criando novos logs de eventos quando os limites de tamanho são atingidos. Os logs de eventos do Windows oferecem informações forenses valiosas.
- **Plano de resposta a incidentes:** desenvolva, implemente, teste e mantenha um plano de resposta a incidentes de segurança cibernética para a organização. Revise e teste regularmente o plano, atualizando e refinando seu conteúdo conforme necessário.
- **Gestão de ativos de hardware e software:** implemente a gestão de ativos de hardware e software em toda a organização. Incorpore índices de priorização e criticalidade na solução de gestão de ativos para identificar rapidamente os ativos de alto valor. Mantenha um inventário atualizado de ativos de hardware e software, o que vai ajudar a identificar possíveis riscos e possibilitar a formulação de planos estratégicos para lidar com esses riscos.

- **Topologia de rede:** mantenha um diagrama atualizado e de alto nível da topologia da rede da organização, para servir como referência para a revisão de configurações existentes e tipos de infraestrutura e ajudar a formular planos estratégicos para alterações e implementações de rede. Durante um ataque à segurança cibernética, o diagrama da topologia de uma rede pode ajudar a equipe de resposta a incidentes no entendimento da estrutura organizacional da rede, permitindo que ações direcionadas de resposta a incidentes sejam executadas com maior precisão e rapidez.

Integridade de dados

Backups:

- Proteja dados de backup implementando uma variedade de soluções de backup, armazenando dados de backup em locais totalmente segregados e usando tipos de mídia independentes do patrimônio corporativo, e gerenciando o acesso com os controles de segurança apropriados.
  - Comece a formular suas soluções de backup redundante seguindo a regra 3-2-1 e aplicando a criptografia adequada aos dados de backup em repouso: crie 3 cópias dos dados, armazene os dados em pelo menos 2 tipos de mídia diferentes e guarde 1 cópia dos dados em uma localidade física separada.

Criptografia:

- Implemente a criptografia completa de disco, dispositivos móveis e unidades USB para proteger os dados contra o acesso não autorizado nos casos de perda ou roubo do dispositivo.
- Proteja os dados em repouso na organização implementando a criptografia DARE (Data At Rest Encryption), priorizando os dados altamente confidenciais. Assegure-se de que os mecanismos de criptografia sejam aplicados aos dados da rede em trânsito, usando a versão mais recente do protocolo TLS (Transport Layer Security) para comunicar as trocas criptografadas envolvendo certificados digitais e prevenindo os servidores de fazer o downgrade de pacotes de códigos para acomodar os tipos de navegadores sem suporte.

Investimentos em segurança

Use as lições aprendidas com os incidentes de segurança para justificar fundos e melhores orçamentos para aplicar à postura de segurança da organização.

- Invista no treinamento e conscientização dos funcionários. Como os humanos costumam ser o vetor inicial dos ataques, invista em:
  - Treinamento e conscientização sobre phishing ou soluções que eduquem e testem os usuários finais sobre as técnicas comuns de phishing. Integre esse treinamento na empresa como um exercício contínuo seguindo implementações agendadas ou simulações de ataque automatizadas e fornecendo os relatórios necessários para a equipe de TI traçar um retrato das vítimas mais comuns e oferecer orientações adequadas.
  - Capacitação dos funcionários em segurança de TI, particularmente nos campos de análise de segurança, caça a ameaças e resposta a incidentes.

Serviços de segurança cibernética gerenciada

- Contrate profissionais de segurança cibernética especializados em análise de segurança, caça a ameaças, resposta a incidentes, engenharia de detecção e ferramentas de segurança etc. Implementar um centro de operações de segurança cibernética permite que a empresa monitore e responda às ameaças 24 horas diárias.
- Invista em uma solução de segurança cibernética gerenciada, como o Sophos Managed Detection and Response (MDR). Os serviços MDR são operações de segurança terceirizadas fornecidas por uma equipe de especialistas que atua como uma extensão da equipe de segurança do cliente.

Investimento em ferramentas

- Sophos XDR – Extended Detection and Response – é uma solução que armazena e capacita a consulta de informações críticas do endpoint, servidor, firewall, e-mail e outros produtos habilitados para XDR, agilizando os fluxos de trabalho de detecção e resposta a ameaças.

- A tecnologia SIEM (Security Information and Event Management) oferece funcionalidades de detecção de ameaças, conformidade e gestão de incidentes ao reunir eventos e informações de várias fontes de dados em um repositório centralizado de dados sobre ameaças.
- Investimentos adicionais podem ser feitos com base nos ensinamentos adquiridos e devem incluir melhorias à postura de segurança medida pelo fechamento das lacunas em proteção, filtragem, detecção e monitoramento. As ferramentas podem incluir AV, sistemas IPS/IDS de prevenção/detecção de invasão, firewalls etc.

Ao tratar das melhorias a essas áreas comuns, a sua organização pode aprimorar sua postura de segurança significativamente e se proteger melhor contra futuros incidentes cibernéticos. Lembre-se de que as lições aprendidas são um processo contínuo, e que revisar e atualizar regularmente as suas práticas de segurança ajudará a sua organização a se manter resiliente diante da evolução das ameaças cibernéticas.

Relatório de incidentes

Ao encerrar o processamento de um incidente, é vital informar os detalhes, descobertas e passos de remediação a todas as partes envolvidas. Notificar um incidente internamente, às autoridades regulatórias e às autoridades legais é essencial para manter a transparência, garantir a conformidade e apoiar as investigações.

Relatórios internos

Para fomentar uma cultura de melhoria e aprendizado contínuos, as organizações devem estabelecer um processo claro de relatórios internos. Esse processo deve incluir:

- Documentação do incidente, incluindo o cronograma dos eventos, os sistemas afetados e a natureza do ataque.
- Resumo do impacto do incidente nas operações, finanças e reputação da organização.
- Descrição dos passos seguidos para conter, erradicar e recuperar-se do incidente.
- Identificação das lições aprendidas e recomendações para futuras melhorias à postura de segurança da organização.
- Envio do relatório do incidente às partes envolvidas relevantes, como gerência sênior, equipes de TI e funcionários e departamentos afetados.

Notificação às autoridades reguladoras

Dependendo da jurisdição e do setor, as organizações têm a obrigação de informar as autoridades reguladoras sobre incidentes de segurança cibernética. Conformar com suas exigências é essencial para evitar multas, penalidades e danos à reputação da organização. Ao informar as autoridades reguladoras, as organizações devem:

- Determinar a autoridade ou autoridades apropriadas para notificar, de acordo com a natureza do incidente e a localização e o setor de atuação da organização.
- Revisar as exigências relevantes constantes no relatório, incluindo as informações necessárias e o prazo de notificação.
- Preparar um relatório detalhado de acordo com o formato exigido e fornecendo o conteúdo especificado pela autoridade reguladora.
- Enviar o relatório dentro do prazo especificado e manter um canal de comunicação aberto com a autoridade reguladora durante todo o processo de investigação e resolução.

Notificação às autoridades legais

Nos casos de atividades criminosas ou ataques cibernéticos significativos, as organizações devem notificar o incidente às autoridades legais. Isso pode ajudar nas investigações e levar à detenção dos hackers. Ao informar as autoridades legais, as organizações devem:

- Identificar a agência ou agências apropriadas, como polícia local, unidades de segurança nacional contra crimes cibernéticos ou agências especializadas (a Polícia Federal, por exemplo).
- Reunir indícios suficientes, incluindo logs, imagens de sistemas e capturas do tráfego da rede, enquanto mantêm a cadeia de custódia e aderem aos requisitos legais aplicáveis.
- Preparar um relatório minucioso do incidente, incluindo a natureza do ataque, os dados e sistemas afetados, o cronograma dos eventos e todas as informações conhecidas sobre os invasores.
- Cooperar com as autoridades legais durante toda a investigação, fornecendo informações adicionais e assistência sempre que necessário.

Seguindo essas diretrizes ao notificar um incidente, as organizações, além de garantirem a transparência e o cumprimento dos requisitos regulatórios, também apoiam os esforços conjuntos de combate ao crime.

Conclusão

Em linhas gerais, este guia de planejamento de resposta a incidentes oferece uma estrutura ampla para as organizações se prepararem com eficiência para gerenciar e se restabelecer de incidentes de segurança cibernética. Ao implementar uma gestão proativa e precauções de segurança, assegurar a integridade dos dados, investir no treinamento de funcionários e em ferramentas de segurança e estabelecer procedimentos claros de relatório, as organizações podem melhorar significativamente sua resiliência contra as ameaças cibernéticas.

O planejamento eficiente de resposta a incidentes não apenas ajuda as organizações a minimizar os danos causados pelos ataques cibernéticos, mas também fomenta uma cultura de melhoria e aprendizado contínuos. Para acompanhar a evolução do panorama de ameaças cibernéticas, as organizações devem revisar e atualizar regularmente seus planos de resposta a incidentes para se manterem na dianteira das vulnerabilidades e ameaças emergentes.

Seguindo atentamente as diretrizes dispostas neste guia, as organizações podem se equipar melhor para detectar, conter e remediar incidentes de segurança cibernética, proteger seus bens e dados valiosos, seguir a conformidade regulatória e conservar sua reputação em um mundo altamente interconectado.

Para obter mais informações sobre o serviço Sophos Incident Response, clique aqui

Enfrentando uma violação ativa?

Ligue para o telefone de contato regional abaixo e fale com um dos nossos consultores de incidentes.

Austrália: +61 272084454

Áustria: +43 73265575520

Canadá: +1 7785897255

França: +33 186539880

Alemanha: +49 61171186766

Itália: +39 0294752897

Países Baixos: +31 162708600

Suécia: +46 858400610

Suíça: +41 445152286

Reino Unido: +44 1235635329

EUA: +1 4087461064

E-mail: RapidResponse@Sophos.com

Nossos consultores de incidentes entrarão em contato o mais rápido possível.

2023-07-03 (IRG-MP)

SOPHOS