ZURICH

Plano de Resposta a Incidentes (IRP)

Plano de Resposta a Incidentes

Introdução

Gestão de incidentes são as ações que uma empresa toma para prevenir ou conter o impacto de um incidente enquanto este está ocorrendo ou brevemente após ter ocorrido (NIST). O processo de resposta a incidentes deve estar muito bem alinhado às políticas estabelecidas e aos objetivos de negócios da companhia.

Principais fases

Todo documento de Plano de Respostas a Incidentes deve possuir as principais fases listadas abaixo:

Preparação: como estar preparado e agir diante de um incidente?

Identificação: quais os critérios de identificação de incidentes?

Contenção: como conter o incidente?

Erradicação: como eliminar a causa-raiz do problema?

Recuperação: o que fazer para restabelecer a normalidade de todos os sistemas?

Lições aprendidas: o que fazer para que os mesmos erros não ocorram novamente?

Preparação

Como estar preparado e agir diante de um incidente?

- Formalize, treine e capacite a equipe que atuará no incidente. Analise o conhecimento técnico/comportamental necessário da equipe.
- Discrimine as funções de cada integrante. As funções e responsabilidades devem ser definidas em toda a organização para identificar, detectar, analisar, conter e responder os incidentes.
- Mantenha uma lista atualizada dos principais contatos para serem acionados. Ex: departamentos, seguradora, corretora, prestadores de suporte no incidente etc.
- Elabore uma diretriz sobre quem deve ser notificado para determinado assunto e em qual janela de tempo. Lembre-se de manter a lista de contatos atualizada.
- Mantenha treinados os principais envolvidos no plano.
- Verifique quais são os processos necessários para a atuação no caso de um incidente. Faça um levantamento de quais já estão implementados e quais precisam de ajustes (ausência de atividades ou serviços, fluxos mal definidos, gargalos etc.).
- Faça um levantamento de quais são os ativos críticos da sua empresa, quais são as vulnerabilidades, os tipos de incidentes mais recorrentes e quais respostas seriam necessárias para cada um deles.
- Elabore play books/cenários para o tratamento de ameaças específicas. Ex: infecção vírus/malware, ataque de ransomware, extorsão, vazamento de dados pessoais, vazamento de dados do negócio/dados confidenciais, ataque DDoS etc.
- Defina qual será a sua estratégia de comunicação/notificação para cada tipo de incidente. Esta, por sua vez, deve estar alinhada à estratégia e às políticas da empresa.
- Oriente como os dados devem ser processados e manuseados, garantindo sua disponibilidade, integridade e confidencialidade. Lembre-se: os dados de incidentes devem ser protegidos por questões legais, necessidade de negócio e ameaça de potencial invasão.

- Disponibilize fluxos/políticas/modelos aprovados e disponíveis para:
  - funcionários relatarem atividades suspeitas;
  - processo de escalonamento de incidentes;
  - políticas internas que contribuam para resposta dos incidentes;
  - ativos críticos da sua empresa, quais as vulnerabilidades encontradas neles e como seriam as respostas ao incidente, caso ocorra;
  - modelos de comunicação interna;
  - modelos de comunicação externa;
  - política de descarte de dados;
  - protocolo de comunicação de sinistro da seguradora.
- Defina como serão os testes do Plano de Resposta a Incidentes e em qual periodicidade ele ocorrerá.

Identificação

Quais os critérios de identificação de incidentes?

- Elabore um processo de identificação do incidente, para que seja determinado se ele é realmente um incidente de segurança.
- Determine quais são as fontes de detecção que a empresa possui. Identifique como os incidentes atuais são detectados e relatados, quem executa funções como gerenciamento de vulnerabilidades, avaliações de risco, monitoramento e controle de rede. As fontes de detecção podem ser humanas, internas e externas.
- Elabore uma tabela de triagem/fluxo a ser seguido após um incidente confirmado. Essa tabela servirá de guia para que seus colaboradores saibam como agir e quais passos devem ser seguidos. Dessa forma, ela contribuirá para uma resposta mais rápida, eficiente e adequada ao incidente.
- Elabore um fluxo de escalonamento de incidentes, de acordo com o tipo e a criticidade, a fim de que a equipe possa usá-lo durante o processo.
- Cada incidente possui um tipo de resposta inicial a ser adotado de acordo com a sua criticidade. Desse modo, inclua na sua tabela de triagem as possíveis respostas, de acordo com o incidente. Confira as sugestões a seguir!

  Tipos de resposta

  - Resposta técnica: em que uma equipe técnica, com foco em resolver o incidente, analisa informações, como o código malicioso e maneiras de mitigar o incidente, assim como o de recuperar o ambiente. Atua também na erradicação, ou seja, na eliminação/limpeza dos arquivos maliciosos.
  - Resposta administrativa: deve garantir que as diversas áreas atuem em conjunto e em sinergia com o fluxo de respostas do incidente.
  - Resposta legal: ações relacionadas à investigação, à privacidade, a processos, à imagem etc.

Contenção

Como conter o incidente?

- A fase de contenção deve focar em ações rápidas e imediatas, de forma a retirar o acesso indevido ou limitar a extensão de um ataque.

- Na fase de investigação do incidente para a devida contenção, lembre-se de manter a integridade das evidências para a devida cadeia de custódia forense.
- Tenha em mãos os modelos de comunicações interna e externa, para estas serem utilizadas no caso de um incidente, visando à comunicação imediata aos principais envolvidos internos e externos, de modo que estes ajam assim que forem recebidas essas comunicações. Ações como essa podem evitar que o incidente se alastre ainda mais.

Erradicação

Como eliminar a causa-raiz do problema?

- A fase de erradicação deve garantir a eliminação da causa-raiz do problema.
- Analise o que deve ser realizado, para garantir a continuidade dos negócios.
- Corrija os sistemas afetados e faça as atualizações necessárias.
- Nem sempre essa fase deve ocorrer antes da fase de recuperação. Às vezes, ambas acontecem juntas. Veja abaixo as dicas para restaurar e recuperar os sistemas.

Recuperação

O que fazer para restabelecer a normalidade de todos os sistemas?

- Focar esforços para restaurar os sistemas afetados, garantindo sua integridade.
- Desenvolver processo de reativação dos ambientes afetados, nos quais constem a ordem correta dos processos/sistemas a serem disponibilizados novamente.
- Retornar os sistemas afetados ao ambiente de produção somente após testes e validações, para garantir que nenhuma ameaça permaneça.
- Instalar os patches e atualizações nos sistemas de segurança, roteadores e firewalls.
- Reinstalar sistemas operacionais de máquinas afetadas.
- Alterar senhas de usuários e administradores locais dos equipamentos afetados e, caso identificado o uso de credenciais privilegiadas, estas devem ser bloqueadas.
- Realizar scan de vulnerabilidades em todas as máquinas afetadas ANTES de conectá-las novamente na rede.
- Monitorar de perto os sistemas, após reconectados à rede.
- Realizar pentestes nos sistemas afetados ou explorados pela ameaça.
- Restaurar sistemas utilizando backups íntegros e não afetados pelo incidente.

Post-mortem/lições aprendidas

O que fazer para que os mesmos erros não ocorram novamente?

- Um exercício de lições aprendidas deve ser realizado com todos os envolvidos nos ciclos de resposta a incidentes, de modo a atualizar o plano com possíveis melhorias encontradas. Essa prática é de extrema importância, pois, com ela, podemos identificar possíveis necessidades de mudanças nos processos internos e melhoria no processo de resposta a incidentes. Esse é um bom indicador para conseguir investimento de correções nas vulnerabilidades.
- Analise se é possível achar a causa-raiz dos incidentes em comum.

- Elabore um modelo de relatório para ser utilizado com template, para que perguntas estratégicas sejam respondidas.
- Elabore um relatório de fechamento do incidente (veja modelo mais abaixo). Esse deve conter:
  - quem elaborou o relatório;
  - qual foi o incidente;
  - detalhes do incidente;
  - detalhes das consequências;
  - detalhes das ações tomadas;
  - como foi o processo de recuperação;
  - processo de revisão;
  - lições aprendidas;
  - plano de melhorias a serem aplicadas.
- Verifique a necessidade de treinar funcionários, terceiros, fornecedores e pessoas envolvidas no plano, para que o erro do incidente não ocorra novamente.
- Elabore um exercício de lições aprendidas e atualize o plano de resposta a incidentes com as informações relevantes.

Dicas adicionais

Documente e mantenha a rastreabilidade

- É fortemente recomendado que todo o processo de atuação no incidente seja documentado, de forma a garantir que toda informação coletada e as ações tomadas fiquem registradas para futuras consultas. Exemplos:
  - coleta e preservação de dados;
  - comunicações;
  - notificações;
  - análise preliminar;
  - resposta preliminar;
  - contenção:
  - erradicação;
  - recuperação;
  - resolução;
  - pós-incidente.

Pratique periodicamente

Você acredita que o seu processo de gestão de incidentes está funcionando? Alguma vez já realizou um exercício prático para analisar como a equipe reagiria diante de um incidente?

Normalmente, essa fase é muito negligenciada pelas empresas. Infelizmente, a falta de prática prejudica muito quando ocorre um incidente, fazendo com que, muitas vezes, a proporção deste seja maior do que se a companhia estivesse preparada, treinando seus funcionários esporadicamente sobre como agir no caso de um incidente.

É sabido que, quando ocorre um incidente de segurança, as primeiras 48 horas são determinantes para se mitigar o impacto que este causará. Logo, uma empresa preparada para agir corretamente desde a detecção de um incidente reduzirá prontamente grande parte do impacto causado por ele.

Boas práticas de mercado sugerem que o IRP seja testado trimestralmente com exercícios de mesa (table top). Além dessa metodologia, há também o exercício de simulações “ao vivo”, o qual demanda mais tempo, esforço da companhia e de seus funcionários, mas é extremamente importante que ocorra de forma semestral ou anual.

Você sabia?

Você sabia que há no mercado excelentes ferramentas de SOAR (Security Orchestration Automation and Response) para contribuir na orquestração e automatização do processo de resposta a incidentes?

Exemplo de template para relatório pós-mortem

Elaborado por:	Nome, data, departamento, e-mail e telefone.
Qual foi o incidente?	Relatar o incidente.
Detalhe o incidente	Como aconteceu? Quando? Quando foi descoberto? Quem descobriu o incidente? Como se descobriu o incidente?
Detalhe as consequências	Quais sistemas foram afetados? Possui correlação com outros incidentes? Se sim, especifique: Quais foram os impactos do incidente?
Detalhe as ações	Quais medidas foram tomadas para conter ou controlar a violação? Quais áreas foram envolvidas na investigação do incidente? Quais foram os planos de comunicações interna e externa adotados?
Recuperação	Qual foi o tempo de resposta/restauração?
Revisão/lições aprendidas	Quais foram os resultados da investigação do incidente? Quais foram os planos e resultados de contenção, correção e erradicação do incidente? Que mudanças serão implementadas para prevenir ou reduzir o risco ou uma recorrência? Potenciais vulnerabilidades ainda existem? Quais as recomendações técnicas sugeridas? Quais as ações mitigatórias sugeridas?
Plano de melhorias a serem aplicadas:	Novos hardware ou software são necessários? Planos de patch ou atualização? Planos de treinamento (técnicos, usuários finais etc.)? Recomendações de mudança de política ou procedimento? Recomendações para mudanças no Plano de Resposta a Incidentes? Recomendações de comunicações regionais?

Referências

- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-92, Guide to Computer Security Log Management
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-61 r2, Computer Security Incident Handling Guide
- ISO / IEC 27035: Information technology — Security techniques — Information security incident management

Zurich Brasil Seguros
Av. Jornalista Roberto Marinho, 85 - 23º andar
Brooklin Novo – 04576-010
São Paulo, SP – Brasil

Publicação do Departamento de Risk Engineering da Zurich Brasil Seguros S.A.
Edição digital nº 39 – atualizada em junho/2021

Para receber outros informativos ou obter maiores informações, contatar o Departamento de Risk Engineering da Zurich.

E-mail: engenharia.riscos@br.zurich.com

ZURICH®