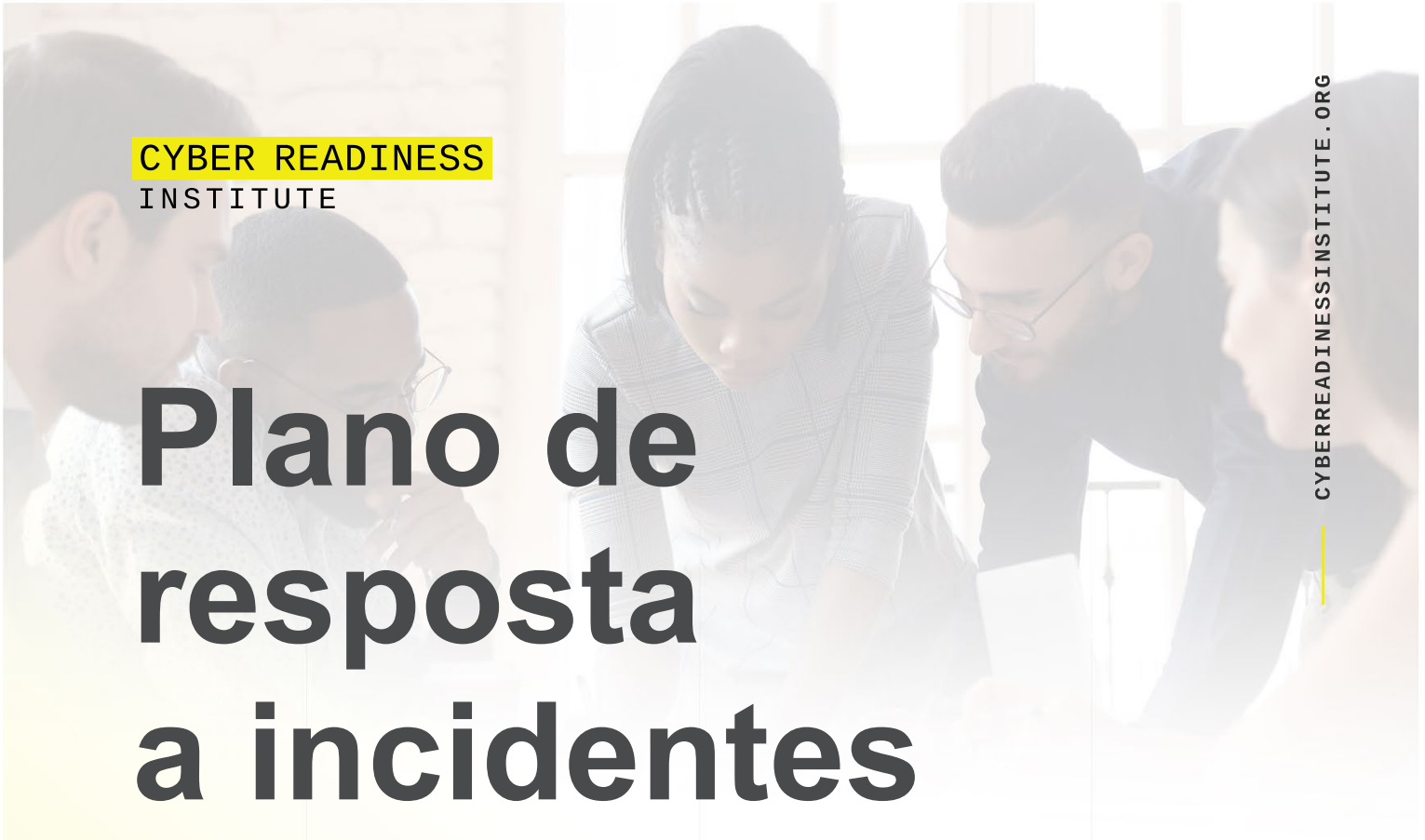

CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Plano de resposta a incidentes

Responder eficazmente aos problemas cibernéticos

Estabelecer práticas e políticas de prontidão cibernética ajuda a reduzir o risco, mas é importante assumir que a nossa empresa irá provavelmente enfrentar a qualquer momento um incidente de segurança que poderá ter impacto nas operações empresariais. Tentar determinar como responder durante um incidente não é boa ideia. O tempo de resposta é fundamental para minimizar os danos. Dispor de um plano bem definido pode fazer a diferença entre um incidente e uma catástrofe.

Visão geral

Um Plano de resposta a incidentes abrangente e gradual equipa-nos para podermos responder, corrigir e aprender rapidamente com todos os incidentes. Este Plano de resposta a incidentes funciona como um roteiro para o que fazer quando se responde a um incidente de segurança, assegurando que damos uma resposta estratégica e não apenas uma resposta reativa.

A nossa resposta a incidentes inclui três elementos principais:

1. **Preparar** para um possível incidente no futuro
2. **Responder** durante o incidente
3. **Recuperar** do incidente

Como se preparar

Diretrizes organizacionais:
Tal como em muitas outras circunstâncias, um pouco de preparação faz uma grande diferença. Existem alguns elementos de resposta essenciais que devem ser realizados o mais brevemente possível para se preparar para os danos causados por um ataque e os reduzir.

1. **Faça cópias de segurança dos dados e certifique-se de que consegue voltar a instalar os dados a partir das cópias de segurança.** A recuperação de um ataque será muito mais rápida e afetará muito menos as operações se tiver cópias de segurança atualizadas do software do sistema, das aplicações e, sobretudo, dos dados importantes. Também deverá assegurar que todas as pessoas na sua organização têm cópias de segurança, caso este processo não esteja centralizado. É importante testar regularmente as suas cópias de segurança.

    - ✓ Data de conclusão: [DATA]

2. **Assegure que todos sabem reportar um possível incidente.** A deteção atempada é muitíssimo importante. Todos os membros da equipa devem conseguir identificar atividades suspeitas e saber quem contactar nesta eventualidade.

    - ✓ Contacto designado de incidente interno: [DETALHES DE CONTACTO]
    - ✓ Data de conclusão: [DATA]

3. **Obtenha um bom apoio técnico externo para a resposta ao incidente.** Saiba a quem se dirigir e como os contactar em caso de emergência. Um incêndio que não consigamos controlar obriga a chamar os bombeiros. Tem de saber a quem deve pedir apoio se um incidente cibernético estiver fora da sua capacidade de controlo. No mínimo, deve tratar-se de um especialista em apoio de TI que conheça e em quem confie. Dependendo do tamanho e da natureza da sua empresa, é sensato identificar os elementos de comunicação adicionais e o apoio jurídico.

    - ✓ Contacto designado de incidente externo: [DETALHES DE CONTACTO]
    - ✓ Data de conclusão: [DATA]

Como responder

Algo de estranho está a acontecer com o computador de um colaborador, que não sabe o que fazer. Isto equivale a sentir o cheiro a fumo ou detetar uma chama pequena na sala de café.

O que deve fazer:

1. **Isole o problema** – retire imediatamente o dispositivo da rede
2. **Identifique o tipo de incidente** e tome a seguinte medida:
    - ✓ Malware: retire imediatamente o dispositivo da rede
    - ✓ Roubo de credenciais – desative mas não elimine a conta e redefinia a palavra-passe
    - ✓ Violação de dados – ligue para o contacto de emergência de TI
    - ✓ Ransomware: retire imediatamente o dispositivo da rede
    - ✓ Recusa de assistência – contacte o seu gestor/TI/Fornecedor de serviços de Internet
3. **Determine o âmbito** do incidente ao colocar estas perguntas:
    - ✓ Quando é que o incidente ocorreu?
    - ✓ Quem foi afetado?
    - ✓ Qual é a natureza técnica do incidente? Como é que ocorreu?
    - ✓ Quem está a par do incidente?
    - ✓ Ainda está a decorrer?
4. **Determine se pode ser controlado internamente de forma adequada** ou se precisa de contactar o suporte de TI externo para assegurar que a falha de segurança é resolvida de forma adequada.
5. **Continue a avaliar se o problema volta a ocorrer.** Caso seja pouco claro se o problema foi resolvido, peque por excesso e contacte um especialista para obter suporte.

Como recuperar

A crise passou e chegou o momento de as coisas voltarem ao normal. O âmbito do incidente e a gravidade do impacto determinarão quanto tempo e esforço serão necessários para a recuperação. No entanto, os passos básicos são os mesmos.

O que deve fazer.

1. Notifique todas as partes afetadas
2. Reponha o ID de utilizador e a palavra-passe do dispositivo comprometido
3. Aplique correções a todos os dispositivos
4. Volte a instalar o software e os dados a partir das cópias de segurança conforme necessário

Lista de verificação de resposta a incidentes

Esta lista de verificação serve para ajudar o gerente de TI ou Líder cibernético

Preparar

1. Faça cópias de segurança diariamente
    - ✓ **Configuração/confirmação de cópia de segurança automática: [DATA]**
2. Teste as cópias de segurança de três em três meses
    - ✓ **Data da última conclusão: [DATA]**
3. Comunicado de protocolo de IRP à força de trabalho
    - ✓ **Data da última conclusão: [DATA]**

O contacto de emergência de TI é: _____
O fornecedor de serviços da Internet é: _____
O contacto de emergência jurídica é: _____
O contacto de emergência de comunicações é: _____

Responder

1. Isole o problema: retire o dispositivo da rede
2. Identifique o tipo de incidente
    - ☐ Roubo de credenciais
    - ☐ Ransomware
    - ☐ Malware
    - ☐ Negação de serviço
    - ☐ Perda de dados confidenciais
3. Determine o âmbito do incidente
    - ☐ Quem sofreu o impacto?
    - ☐ Quando começou o incidente?
    - ☐ Ainda está a decorrer?

Recuperar

1. Notifique todas as entidades
2. Reponha o ID de utilizador e a palavra-passe do dispositivo comprometido
3. Corrija todos os dispositivos
4. Volte a instalar o software e os dados a partir das cópias de segurança conforme necessário

Orientação adicional para a resposta aos incidentes

Esta orientação destina-se ajudar o gestor de TI ou Líder cibernético

Se pretende ter um Plano de resposta a incidentes ainda mais robusto para a sua organização, encontrará abaixo uma abordagem em quatro passos para o efeito, baseada nas orientações do Instituto Nacional de Normas e Tecnologia (NIST - National Institute of Standards and Technology). Poderá não ser totalmente exequível para si seguir todos os passos, mas faça o possível para agir em cada um dos quatro passos de forma a fazer sentido para si e para a sua organização.

1 Preparação

A preparação é fundamental para uma resposta rápida. Neste passo, irá compilar uma lista dos seus recursos, aquilo que faz a sua empresa funcionar. Esta lista incluirá, entre outros, servidores, redes, aplicações e pontos terminais críticos (tais como portáteis). Depois de ter compilado a sua lista de recursos, classifique-os por nível de importância. Em seguida, monitorize os seus padrões de tráfego para conseguir criar linhas de base que pode usar posteriormente para comparação - ou contrate um fornecedor para monitorizar os padrões de tráfego, caso os seus recursos o permitam. Se não puder contratar um fornecedor, uma lista de recursos e dar atenção prioritária aos mesmo é um bom primeiro passo. Crie um plano de comunicações, com orientação sobre quem contactar, como e quando baseado em cada tipo de incidente. Não se esqueça de ligar a todos os contactos desta lista antes de ocorrer uma crise. Um refrão comum no âmbito da gestão de crises é: "Nunca devemos trocar cartões de negócios durante uma crise." Certifique-se de que todas as pessoas na sua lista sabem o que espera delas durante uma crise.

Determine quais são os eventos de segurança passíveis de desencadear o seu plano de resposta a incidentes, e quais são os limiares inferior e superior destes eventos. Para ajudar a identificar os limiares, reflita sobre as situações que poderiam perturbar as suas operações comerciais.

Depois de identificar estes limiares, crie um plano de resposta a incidentes para cada tipo de incidente. O plano pode ser melhorado através de simulacros que permitem identificar lapsos no seu processo, mas também pode ser aperfeiçoado na sequência de eventos concretos (voltaremos a este aspeto mais tarde). O essencial é estabelecer um processo.

2 Deteção e Análise

Neste ponto do processo, identificou-se um incidente de segurança. É neste momento que entramos em modo de investigação. Reúna tudo o que conseguir sobre o incidente. Em seguida, analise os dados. Determine o ponto de entrada e a amplitude da brecha. Este processo torna-se substancialmente mais simples e rápido se todas as ferramentas de segurança de que dispõe estão apontadas numa só localização. Um fornecedor contratado pode executar estas ações por si.

3 Contenção, Erradicação, e Recuperação

A Contenção visa estancar a hemorragia. É nesta fase que fechamos o ponto de entrada da ameaça.

A Erradicação visa remover a ameaça. Se a ameaça obteve acesso a partir de um sistema e proliferou para outros sistemas, terá mais que fazer neste passo.

A Recuperação visa tornar o sistema novamente operacional caso tenha encerrado, ou simplesmente pô-lo a funcionar como habitualmente se nunca tiver encerrado.

4 Lições aprendidas

Este passo oferece a oportunidade de aprender com a experiência para que, em eventos de segurança futuros, possa dar uma melhor resposta. Por mais tentador que seja passar à frente este passo, especialmente com uma lista infindável de coisas a resolver, este passo é vivamente recomendado.

Avalie o incidente com um olhar simultaneamente humilde e crítico para identificar áreas de melhoria. Em seguida, adicione estas melhorias à sua documentação.

Não há um processo perfeito para todos os cenários possíveis. Alguns cenários são inconcebíveis até ao momento em que ocorrem. O atual panorama de ameaças também está em permanente evolução, pelo que o seu processo de resposta a incidentes irá exigir atualizações ocasionais. Lembre-se, o seu futuro eu irá agradecer-lhe. Como seu costuma dizer, "Nunca desperdiçar uma boa crise."