POLÍTICA DE RESPOSTA A INCIDENTES DE SEGURANÇA

1. Contextualização

O Plano de Resposta a Incidentes de Segurança e Privacidade se configura como um procedimento fundamental. Ele delineia o método pelo qual a Catavento Pesquisas irá reagir diante de situações de urgência e circunstâncias excepcionais. Dada a possível gravidade das situações, é crucial que a reação da empresa seja ágil e confiável, ao mesmo tempo em que preserva as evidências que podem contribuir para evitar ocorrências futuras. Isso é feito de acordo com as obrigações legais de comunicação e transparência por meio das etapas descritas neste documento.

2. Início

Um novo incidente é notificado, por pessoa externa ou não à empresa ou por alarme do monitoramento, usando um dos mecanismos de comunicação definidos. Notificação é recebida pelo titular de dados.

3. Triagem

- O titular dos dados deve fazer a avaliação preliminar, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.
- Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravarem se não houver resposta imediata.
- Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para tramites regulares da empresa e notificações.
- Em caso de incidentes que exigem resposta imediata ou melhor avaliação, passamos às fases seguintes.

4. Avaliação

- Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases.

5. Contenção e Erradicação

- O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida será realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas.

- Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot para posterior análise.

6. Recuperação

- A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema.
- Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas.
- Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

7. Lições aprendidas

- Com o incidente contido e sua resolução encaminhada, um documento com lições aprendidas deve ser registrado com as medidas tomadas e recomendações para evitar novo incidente.

8. Documentação

- Todo o processo deve ser documentado deve ser documentado detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas.

9. Comunicação

- Assim que possível, no caso de incidente com vazamento de dados pessoais, a empresa deve avaliar e fazer as comunicações obrigatórias por Lei, se houverem, bem como informar e subsidiar os controladores dos dados. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a ANDP.

Três Coroas, 01 de março de 2023