SIMULADO DE GESTÃO DE CRISE

Como agir em casos de Incidentes Cibernéticos e de Dados Pessoais

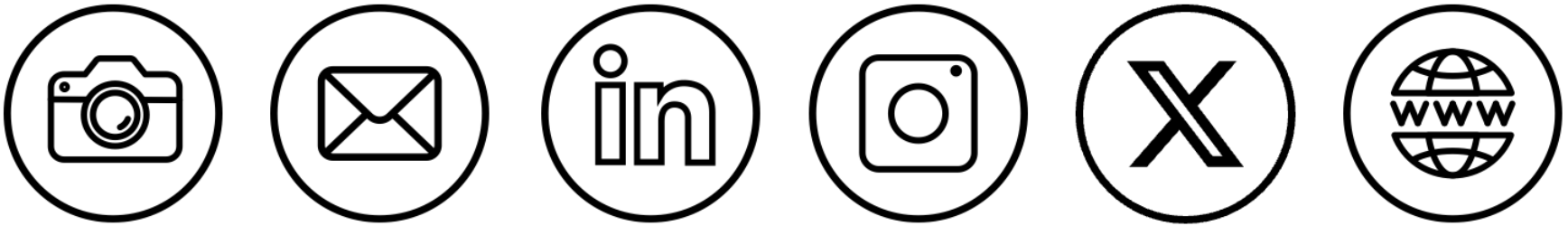
TLP: Clear

Realização Grant Thornton

Parceria Opice Blum

TLP:CLEAR

NÃO HÁ LIMITES NA DIVULGAÇÃO



https://cert.br/tlp/

SIMULADO DE GESTÃO DE CRISE

Abertura

Como agir em casos de Incidentes Cibernéticos com Dados Pessoais

Ataques cibernéticos são cada vez mais frequentes. Esses ataques visam a exploração de vulnerabilidades no ambiente tecnológico de empresas, e podem causar impactos financeiros, operacionais e reputacionais.

Pensando nisso, a Grant Thornton Brasil, em parceria com o Opice Blum Advogados, desenvolveu esta apresentação para abordar, de forma prática, esse assunto tão relevante, por meio de uma simulação de gestão de crise.

SIMULADO DE GESTÃO DE CRISE

Conheça os facilitadores do simulado

Everson Probst

Especialista em combate a crimes cibernéticos, Cibersegurança preventiva e Resposta a incidentes, e Sócio de Cyber Security na Grant Thornton Brasil

Tiago Neves Furtado

Advogado e Coordenador de Proteção de Dados Pessoais e Resposta a Incidentes Cibernéticos e de Privacidade no Opice Blum Advogados Associados

Realização

Grant Thornton

Parceria

Opice Blum

TLP: Clear


Realização
Grant Thornton
Opice Blum
PESQUISA
Qual a percepção de
riscos cibernéticos
das lideranças brasileiras?
Sua opinião é valiosa!
Escaneie o QR Code
e participe da
nossa pesquisa.
TLP: Clear

Contexto

Cenário do incidente

- A XPTO e-commerce é uma empresa brasileira de e-commerce que atende pessoas e empresas, oferecendo soluções de venda online, anúncios e serviços;
- Recentemente, a XPTO também passou a comercializar seus próprios produtos;
- A empresa está em um processo de expansão e busca iniciar um serviço de pagamentos online;
- A XPTO opera em toda a América Latina, com mais de 16 mil colaboradores e uma marca reconhecida no mercado;
- A empresa está se preparando para um IPO, o que exige profissionalização e aprimoramento da governança;
- O ambiente tecnológico da XPTO é gerenciado principalmente por profissionais internos, com a inclusão de fornecedores externos em razão do crescimento recente.

Contexto

Dia 1 - Sexta

Primeiros indicadores

- Às 21h32, o SOC detectou tentativas de acesso não autorizado em um servidor crítico.
- Os chamados de usuários foram registrados e classificadas como de baixa prioridade

Dia 2 - Sábado

Agravamento do incidente

- Às 9h15, o analista da XPTO atendeu 42 chamados.
- Nesta manhã, o SOC reportou ao CTO sobre tentativas de acesso não autorizadas.
- Às 15h, o sistema de pagamentos apresentou erros, iniciando um protocolo de avaliação.

Dia 3 - Domingo

Percepção do incidente

- O gerente de infraestrutura foi notificado sobre problemas de segurança às 11h.
- Às 17h20, a equipe de segurança confirmou um ataque de ransomware que afetou servidores da XPTO.
- Às 20h10, 30% dos usuários perderam acesso aos serviços da empresa.

Dia 4 - Hoje

Formação do comitê de crise

- Após o ataque de ransomware, a XPTO ativou o Comitê de Crise.
- O Comitê foi informado sobre o pedido de resgate do grupo atacante.

Formação do Comitê de Crise

Os membros do Comitê devem ser designados de acordo com as necessidades específicas do cenário de risco. Mas é importante que a área de atuação de cada possível membro esteja previamente indicada no Plano de Resposta da empresa.

A. Liderança Executiva: Membro do Comitê Executivo e tomador de decisão;
B. Tecnologia: Representante da área de infraestrutura e telecomunicações;
C. Segurança: Representante da área de segurança da informação;
D. Jurídico: Representante jurídico interno da XPTO;
E. Comunicação: Representante de comunicação e relações institucionais;
F. Operações: Representante de áreas operacionais críticas
G. Privacidade: Encarregado pela proteção dos dados pessoais (DPO);
H. Compliance e Riscos: Representantes de GRC.

SIMULADO DE GESTÃO DE CRISE

Cenários

TLP: Clear

Cenário 1

Identificação do vetor de ataque

Após início da análise, constatou-se múltiplos vetores de ataques possíveis, incluindo phishing e vulnerabilidades não corrigidas nos sistemas, mas ainda não há conclusão definitiva sobre isto. Entretanto, essa informação é relevante para análise correta do incidente e próximas ações adotadas pelo Comitê de Crise.

Com base nestas informações, o Comitê discute avaliar sobre a priorização das análises, e precisa deliberar:

A. Concentrar-se nos logs de e-mail e alertas de segurança em busca de indícios de *phishing* e análise de logs de conexão para identificar potenciais anomalias e confirmar a hipótese.

B. Priorizar a análise de vulnerabilidades e eventuais *patches* faltantes nos sistemas afetados.

C. Dividir o time para cobrir ambas as frentes simultaneamente, mas com recursos limitados para cada frente de trabalho.

Cenário 2

Comunicação com as partes interessadas

Conforme a análise evolui, em que pese o time técnico ainda não ter resposta sobre o impacto do incidente, foi verificado que o ambiente do TI global foi comprometido.

Há grande preocupação sobre o desdobramento do incidente e a repercussão com as partes interessadas (investidores da XPTO, Diretoria, opinião pública).

Com base nestas informações, o Comitê discute sobre a eventual priorização das análises:

A. Emitir um alerta geral imediato a todos os interessados, incluindo investidores, diretoria e colaboradores, detalhando o incidente e possíveis impactos.

B. Comunicar apenas aos líderes de departamento e partes interessadas relevantes, para evitar pânico.

C. Manter o incidente confidencial até que mais informações estejam disponíveis, para evitar desinformação.

Cenário 3

Estratégia de contenção

A equipe de resposta identificou a exploração de uma vulnerabilidade de sistemas conectados à Internet para abertura de portas e implantação de malwares. Mas ainda há muito o que se fazer para controlar o dano do incidente.

Mesmo com as devidas decisões para erradicar o ataque até o momento, ele continua a se propagar pela rede corporativa. Com isso, sistemas inteiros estão sendo paralisados com a criptografia de arquivos e bases de dados. Infelizmente, não há entendimento claro sobre a forma de propagação do *malware*.

Com base nestas informações, o Comitê deve avaliar entre:

A. Desligar toda a infraestrutura de rede, aceitando o impacto operacional, para interromper a propagação.

B. Identificar e isolar as máquinas infectadas uma a uma, tentando manter a operação o mais normal possível.

C. Manter os servidores em funcionamento para garantir a continuidade da operação.

Cenário 4

Estratégia de erradicação

Com a descoberta da origem do ataque já mapeada e após o devido isolamento dos ambientes comprometidos, o time de resposta inicia o planejamento de medidas para remover completamente o *malware* das máquinas e ambientes afetados, garantindo a erradicação e controle total do incidente cibernético.

Com base nestas informações, o Comitê deve avaliar entre:

A. Formatar e reinstalar ambientes afetados.

B. Remover o *ransomware* dos ambientes afetados usando ferramentas de remoção de *malware*.

Cenário 5

Pedido de resgate

Um e-mail enviado pelo *hacker* foi recebido por diversos funcionários da empresa, avisando que dados serão publicados na Internet caso a companhia não pague 18 Bitcoins no prazo de 24h.

Como "comprovação de procedência", o *hacker* envia uma amostra dos dados, incluindo dados pessoais de clientes (nome, CPF, endereço, dados de consumo e renda) e informações estratégicas da empresa (DRE, plano estratégico e *mockup* de novos produtos ainda não lançados).

Com base nestas informações, o Comitê deve avaliar entre:

A. Realizar o pagamento para evitar a divulgação dos dados.

B. Não responder ao pedido de resgate e aguardar a finalização da determinação da extensão dos danos do incidente.

Cenário 6

Comunicação aos titulares e à ANPD

A XPTO já possui bom entendimento sobre a causa raiz do problema, a vulnerabilidade explorada, as medidas técnicas de contenção e remediação, bem como a quantidade e quais titulares foram afetados. Resta pendente a análise dos tipos de dados expostos e o risco/dano que a exposição desses dados representa aos titulares.

Com base nestas informações, o Comitê deve avaliar entre:

A. Realizar comunicação aberta na Internet e disponibilizar canal de atendimento para os afetados.

B. Comunicar a ANPD e aos titulares, indicando a ocorrência do incidente, suas consequências e o estágio das investigações técnicas.

C. Aguardar a avaliação final do incidente e realizar comunicação complementar em até 20 dias úteis sob a justificativa que somente após a conclusão das análises será possível identificar riscos ou danos aos titulares afetados.

Cenário 7

Lições aprendidas

Com a informação exposta na mídia, a XPTO, enquanto operadora de dados, está recebendo questionamentos de seus parceiros e fornecedores sobre os dados compartilhados de seus clientes, que cobram o cumprimento de cláusulas estipuladas nos termos de privacidade.

O comitê precisa deliberar entre:

A. Realizar uma auditoria interna de segurança completa, potencialmente atrasando outras operações, mas identificando todas as falhas de segurança.

B. Focar na revisão de segurança apenas nas áreas afetadas pelo ataque para acelerar a recuperação.

C. Buscar suporte especializado para realizar a análise de segurança e varredura de vulnerabilidades, adicionando uma perspectiva externa ao custo de exposição potencial.

Discussão Final

Ataques cibernéticos são cada vez mais frequentes.

Pensando na necessidade de treinar os Executivos e os Comitês de Crises dos nossos clientes, a Grant Thornton Brasil e a Opice Blum Advogados Associados, desenvolveram uma metodologia completa de Simulado de Gestão de Crise, considerando as melhores práticas e referenciais metodológicos do mercado.

Capacite sua equipe para agir rapidamente em momentos críticos. Quer saber mais e realizar um simulado personalizado para o seu negócio, entre em contato conosco pelo nosso site:

https://www.grantthorntonbrasil.com.br/exercicio-tabletop

Esperamos ter chamado atenção para a importância da temática e de sua complexidade: nem sempre há decisões corretas!

Nem todo incidente será comunicável à ANPD ou precisará ser reportado aos titulares. Importância pra ter critérios para avaliação dos riscos e dos gatilhos de comunicação.

Existem especificidades caso a caso: podem envolver acionamento de outras autoridades de regulação.

Boa-fé e transparência devem nortear as discussões do Comitê de Crise e as medidas de resposta ao incidente.

TLP: Clear