*Por Thales Cyrino e Rodrigo Leal**

Capítulo VI

A importância de se ter uma estratégia de resposta a incidentes

Sexta-feira, 18 horas, véspera de um feriado prolongado, seu celular toca e, após alguns segundos, você percebe que a empresa onde trabalha sofreu um incidente de segurança, nada está funcionando, ninguém sabe de fato o que ocorreu e neste momento é necessário colocar em prática o Plano de Resposta a Incidentes.

Um incidente de segurança é uma violação ou uma ameaça iminente de violação das políticas de segurança, que visa danificar, roubar dados ou interromper o funcionamento de redes e sistemas corporativos. Há inúmeros tipos de incidentes, como ataques de phishing, malware, comprometimento de e-mail e de propriedade intelectual, ransomware, violação de dados e mineração de criptomoedas. Já a Lei Geral de Proteção de Dados (LGPD) classifica um incidente como qualquer evento que envolva a violação dos dados pessoais dos indivíduos.

A estratégia de Resposta a Incidentes não se limita somente ao Plano de Resposta a Incidentes, mas sim a uma série de ações prévias que incluem investimento em pessoas, processos e tecnologia. Podemos dividir em seis etapas conforme processo detalhado a seguir:

1. Preparação;
2. Identificação;
3. Contenção;
4. Erradicação;
5. Remediação;
6. Lições aprendidas.

Durante a etapa de preparação, deve-se preparar para a possibilidade de ocorrência de um incidente de segurança. Esta etapa é muito importante, pois tudo o que será feito e como será feito devem ser definidos neste momento. Durante esta fase deve ser criado e revisado o plano de resposta a incidentes, devem ser gerados runbooks específicos de acordo com o tipo de incidente de segurança, ou seja, criados roteiros a serem executados para cada tipo de incidente de segurança que possa ocorrer. Durante esta fase é importante testar o plano de resposta a incidentes simulando um sem o conhecimento de todos para validar se o plano de fato será seguido, se os processos estarão de acordo e se as pessoas serão aptas para atuar quando o incidente de fato ocorrer.

Na preparação devem ser realizados exercícios, como simulação de phishing, ransonware e outros que irão ajudar a mapear o nível de conscientização das pessoas e testar o processo de resposta ao incidente.

Na etapa de identificação, o principal objetivo é identificar um incidente de segurança de forma mais breve possível. Para que a identificação seja possível, existe uma série de tecnologias necessárias que, através de coleta e correlação de informações, contribui para uma identificação rápida e eficiente. É nesta fase que algumas respostas precisam ser obtidas: o que aconteceu? Como aconteceu? O que foi exposto?

Após identificado o incidente de segurança, é preciso realizar a contenção para que o incidente não aumente o seu alcance. Alguns exemplos de contenção são: isolamento de rede ou host, criação de novas regras em um firewall, atualização de assinaturas ou regras em um IPS (Intrusion Prevention System), etc.

Na fase de erradicação é necessário, de fato, interromper a ameaça removendo por completo de tudo que foi afetado; no caso de um malware, por exemplo, é necessário removê-lo e garantir que ele não exista em outros lugares do ambiente.

Na etapa de remediação é necessário voltar todo o ambiente para o estado anterior ao incidente, poderá ser necessário restaurar backup, reinstalar sistemas, reiniciar aplicações. O grande desafio desta fase é ter certeza de que tudo está sendo restaurado para um momento antes do incidente, garantindo que tudo voltará a funcionar como esperado.

A documentação de tudo que ocorreu e como foi o tratamento do incidente de segurança é de suma importância.

Esta fase é conhecida como "lições aprendidas" e as informações devem ser utilizadas com o objetivo de melhorar todo o processo de resposta a incidentes.

Quem deve ser envolvido durante um incidente de segurança? Como a empresa deve comunicar ao mercado e, internamente, um incidente? Estas e outras definições são realizadas durante a fase de preparação, em que, por definição, os incidentes de segurança devem ser tratados por uma equipe de profissionais de segurança da informação, tecnologia da informação e executivos. Este time é conhecido como CSIRT (Computer Security Incident Response Team) e o FIRST (Forum of Incident Response and Security Teams), que disponibiliza conhecimento e facilita o entendimento para a montagem de um CSIRT a partir do zero.

No último artigo, publicado na edição anterior, discorremos sobre a evolução e a importância de um SOC, neste momento, pode surgir uma dúvida: "SOC e CSIRT não são a mesma coisa?" Não. Estas duas estruturas são atividades complementares, em que o SOC está focado em monitoração e detecção de ameaças, análise e priorização de alertas e o CSIRT possui um foco no incidente, muitas vezes esta confusão ocorre pois o termo SOC é geralmente empregado como o local ou grupo de pessoas responsável por toda a operação de segurança. Além disso, por restrições estruturais e orçamentárias, as atividades relacionadas a incidentes algumas vezes são compartilhadas entre os profissionais do SOC, mas o perfil dos profissionais e as atividades são complementares.

Sabemos que formar essas equipes não é uma tarefa simples hoje em dia. Devido à falta de mão de obra especializada, muitas organizações não conseguem formar suas próprias equipes internas. Além disso, isso requer um investimento alto e sabemos que a pandemia da Covid-19 enxugou ainda mais os orçamentos e potencializou a dificuldade em evoluir os investimentos destinados à proteção de dados.

Neste sentido, terceirizar o CSIRT com parceiros especializados tem se tornado uma tendência que vem ganhando força no mercado. Ao delegar essa tarefa a especialistas, você poderá contar com profissionais dedicados 24/7 no tratamento de incidentes, antes, durante e depois que eles acontecem, que vão atuar de forma rápida e eficiente, realizando toda a gestão do incidente em conjunto com sua equipe de Segurança da Informação.

Somente por meio de um CSIRT você conseguirá garantir a aplicação das melhores práticas e frameworks do mercado, trabalhando para identificar, mitigar, conter, erradicar e remediar um incidente, para recuperar sua operação e restabelecer os sistemas críticos num curto espaço de tempo, sem que seu negócio sofra prejuízos maiores. A partir das lições aprendidas, esses times especializados te ajudarão a estabelecer novas regras para que, quando determinado tipo de ameaça ocorrer novamente, seja muito mais fácil lidar com ele.

No cenário atual, contar com um time de CSIRT é imprescindível independentemente de ser um time interno ou externo. Esta é uma prioridade que deve estar em pauta nas discussões estratégicas, já que um incidente de segurança pode destruir desde a reputação de um negócio a afetar vidas. A infraestrutura crítica, a velocidade e a eficiência na hora da resposta a um incidente são inversamente proporcionais aos possíveis danos causados.

**Thales Cyrino é técnico em processamento de dados, Administrador de Empresa pela Universidade Anhembi Morumbi e Pós-Graduado em Marketing pela FGV SP, com mais de 20 anos de experiência no mercado de TI, em diversas áreas como: redes, telecomunicações, sistemas de monitoramento, infraestrutura computacional, data center, desenvolvimento de software e cybersecurity. Atualmente trabalha como Diretor de Vendas de Cybersecurity na NTT.*

Rodrigo Leal é graduado e mestre em Engenharia Elétrica. Possui MBA em Gestão de Projetos pela FGV e curso de Gestão de Negócios da Era Digital pela Cesar School e, recentemente, Programa Executivo na StartSe. Atualmente, cursa MBA Executivo de Negócios do Setor Elétrico pela FGV. Desde 2000 atua na área de telecomunicações, TI e tecnologia. Atualmente, é assessor do Diretor de Operação na Chesf, coordenando vários processos da diretoria, incluindo os assuntos relativos à tecnologia operativa. Ocupa ainda a posição de Vice-Presidente do Conselho Diretor da UTC América Latina e a coordenador do Comitê de Tecnologia da Informação e Telecomunicações no CIGRE-Brasil.