Desenvolvendo um plano de resposta a incidentes de segurança que funcione

Uma análise dos dez principais erros do CSIRP (Plano de resposta a incidentes de segurança em computadores)

Destaques

- Violações de segurança são praticamente inevitáveis e podem envolver milhares de registros de dados e custar milhões de dólares
- Um Plano de Resposta a Incidentes de Segurança em Computadores, ou CSIRP, pode ajudar a reduzir os custos e mitigar a gravidade das violações
- Com base na experiência de trabalho com centenas de empresas de todos os tamanhos, a IBM oferece consultoria para construir e manter um CSIRP efetivo

Entender o alto custo das falhas de segurança

Empresas globais com centenas de milhares de funcionários, pequenas empresas negociando na web e organizações do setor público de todos os tamanhos têm uma coisa em comum: suas redes estão quase sempre sob ataque contínuo e seus sistemas corporativos também estão em risco. Além disso, é praticamente inevitável sofrer uma violação de segurança em algum momento.[1]

A gravidade dessa violação será influenciada por muitos fatores; um dos mais importantes é sua própria preparação. De acordo com o Ponemon Institute, o primeiro objetivo é ter uma forte postura de segurança, seguido de um Plano de Resposta a Incidentes de Segurança em Computadores (CSIRP) estabelecido para reduzir o custo de uma violação de segurança.[2]

Como base de sua defesa contra hackers, malware, erro humano e uma série de outras ameaças, um CSIRP é o mapa que orienta sua resposta a um ataque bem-sucedido. Ele deve definir as funções e responsabilidades de todos os respondentes, estabelecer autoridade para tomar as principais decisões e definir os fluxos de comunicação e procedimentos notificação. Sem um CSIRP, sua equipe de resposta a incidentes pode desperdiçar tempo e recursos valiosos para definir quem faz o quê, levando a custos potencialmente maiores e maior dano à sua organização e reputação.

Desenvolvimento de um plano de resposta a incidentes efetivo

Embora os componentes básicos de um CSIRP sejam simples e diretos, elaborar um plano efetivo exige equilibrar meticulosidade e usabilidade. Dado o cenário de ameaças em crescente evolução, não é possível construir um plano que aborde todos os ataques em potencial – nem você desejará um documento tão detalhado e complexo. Ao invés disso, você pode criar diretrizes flexíveis que, de uma forma simples e rápida, podem ser aplicadas a qualquer tipo de incidente.

O pior momento de descobrir que seu CSIRP é falho é durante uma emergência. Ao ajudar clientes a responder a incidentes declarados, os especialistas em segurança da IBM em nossas equipes de Serviço de Resposta a Emergências conseguem observar o que funciona e o que não funciona em um CSIRP. Neste artigo, compartilhamos as dez principais falhas de CSIRPs que encontramos e como você pode evitar esses erros potencialmente onerosos.

1 Tornar um CSIRP complexo demais

Ao projetar seu CSIRP, é melhor ter em mente que o público estará lendo o documento durante uma crise. Haverá estresse, caos e, é claro, urgência. Alguns indivíduos entrarão em pânico e temerão por seus cargos. Os executivos que podem ou não compreender os pequenos pontos técnicos do que está acontecendo se sentirão estressados se a mídia jornalística fizer perguntas.

Os CSIRPs devem ser incisivos, claros e concisos. Se um funcionário que não está familiarizado com o documento não puder rapidamente examinar os processos descritos no CSIRP, compreender a cadeia de comando e realizar as ações necessárias, seu CSIRP pode ser complexo demais. É claro que tornar o CSIRP simples demais também é um risco potencial; obter o equilíbrio certo entre brevidade e direção acionável é essencial para o sucesso de um CSIRP.

Ter um plano de resposta a incidentes estabelecido fez com que organizações americanas economizassem, em média, US$ 1,2 milhões por violação de dados em 2013.[3]

2 Sobrecarregar a equipe principal

Toda organização tem um "Zé". O Zé conhece todo mundo e todos os sistemas, roteadores, cabos e máquinas de café no prédio. O Zé é a pessoa que procuramos durante um incidente. O Zé, incontestavelmente, é a melhor pessoa que se pode ter para os pequenos incidentes, sendo capaz de lidar com eles do começo ao fim. Ao desenvolvermos os CSIRPs para nossos clientes, rapidamente encontramos o "Zé" da organização durante nosso questionamento padrão: Quem é responsável pelo antivírus? O Zé. Quem toma a frente na resposta técnica? O Zé. Quem se comunica com os executivos e autoridades reguladoras? O Zé.

O Zé é fantástico no que ele faz durante um dia normal de serviço. Mas quando um incidente avança durante vários turnos ou mesmo dias, o Zé não pode ser seu "cara" por 72 horas ininterruptas. É necessário separar as obrigações durante um incidente e distribuí-las entre a equipe treinada e designada se uma organização não deseja ter funcionários sobrecarregados, sem dormir – e com isso, menos funcionários atendendo a incidentes.

3 Tratar a resposta a incidentes como um processo em série

Durante um incidente em larga escala, as multitarefas são essenciais. Os gerentes que visualizam uma resposta a incidentes como um processo em série estão fadados a falhar quando precisam resolver um incidente de em tempo hábil. Embora cada incidente seja exclusivo, todas as respostas a incidentes possuem uma série de esforços de curto prazo. Lançar novas assinaturas antivírus, corrigir sistemas, liderar esforços investigativos, informar funcionários e clientes sobre seu status atual, buscar outras fontes de bebidas cafeinadas e outras tarefas importantes são processos individuais e devem ser tratados dessa forma. Uma falha comum é focar somente em uma dessas tarefas por vez e negligenciar outras tarefas importantes que devem ser realizadas em paralelo.

4 Deixar de estabelecer linhas de comunicação adequadas

Ao responder a um incidente, é provável que a ajuda de vários indivíduos e fornecedores diferentes seja solicitada. O indivíduo responsável por gerenciar os "eventos em solo" – o gerente de incidentes – deve ser um mestre de comunicações. A comunicação deve ser ordenada, eficiente e seguir os canais adequados para garantir que todas as partes envolvidas na resposta sejam mantidas informadas e coordenadas. Dentro de uma organização, isso poderia incluir equipes técnicas além daquelas responsáveis pela segurança física, recursos humanos, conformidade, assuntos regulatórios e gerenciamento de risco. As comunicações externas também são cruciais, exigindo que alguém seja claramente designado como responsável por fornecer atualizações oportunas e concretas para os pontos focais de relações públicas, relações com a mídia, relações com o cliente e marketing de sua organização. Muitas vezes uma organização quebra a confiança das partes interessadas ao deixar de comunicar de forma rápida e aberta sobre os incidentes de segurança.

5 Focar no que é fácil, não no que precisa ser feito

Durante quase todos os incidentes, surge o desejo de focar nas tarefas simples ao invés do que precisa ser feito. Isso é o mesmo que abastecer o líquido de limpar para-brisas no carro quando o motor não pega. Ao resolver um incidente de segurança, é tentador focar muita atenção nas tarefas fáceis, como coletar evidências estáticas – por exemplo, capturar imagens do disco rígido – ao invés de tarefas mais desafiadoras, como executar análises. Mas independente da dificuldade, todas as tarefas precisam ser concluídas. Deixar de focar sua energia nos problemas essenciais, sejam eles fáceis ou difíceis, somente causará mais dores de cabeça e incidentes mais prolongados.

Pelo menos 50 por cento dos CSIRPs avaliados pelos consultores de segurança da IBM não apresentaram nenhuma evidência de um ciclo de vida formal de documentos ou um histórico de revisões contínuas.

6 Focar no que é interessante, não no que precisa ser feito

Durante alguns incidentes, o respondente descobrirá algumas informações interessantes e se tornará focado em buscar um caminho não relacionado. Uma fonte comum de desvio é encontrar atividades de usuários inadequadas, como navegar em sites que estão fora dos limites. Essas informações recentemente descobertas podem ser extremamente cativantes, mas se não tiverem uma função material importante no incidente que você está investigando, deverão ser deixadas de lado para pesquisa posterior. Horas infindáveis podem ser gastas nesse desvio, consumindo tempo que você não pode dar o luxo de perder. Continue focado na resolução do incidente e deixe a exploração para mais tarde.

Conselhos da IBM para os primeiros respondentes

Mantenha essas dicas em mente quando um incidente de segurança for declarado.

FAZER:

- Consultar e seguir o CSIRP da sua organização
- Reunir inteligência de incidentes de várias fontes
- Assegurar que as pessoas adequadas estejam envolvidas
- Começar a fazer anotações minuciosas de primeiro respondente
- Ativar as credenciais de Respondentes de Incidentes únicos
- Coletar dados voláteis e arquivos de log pré-determinados
- Proteger sistemas e mídia para investigação forense
- Coletar logs baseados na rede para análise futura

NÃO FAZER:

- Entrar em pânico ou reagir sem um plano
- Discutir o incidente com outros a menos que devidamente instruído
- Desligar, encerrar ou fazer o backup dos sistemas afetados
- Acessar sistemas remotamente a menos que necessário
- Usar credenciais de domínio privilegiado comuns
- Instalar ou executar qualquer software nos sistemas
- Realizar processos de varredura de antivírus ou semelhantes
- Tentar retaliar os perpetradores

---

7 Abandonar o CSIRP

Ocasionalmente surgirá o desejo de jogar o CSIRP fora pois ele não atende a situação específica apresentada. Há um motivo para o documento não endereçar o vírus de e-mail ou cavalo de troia mais recente. O CSIRP não é um guia completo sobre como abordar cada tipo específico de incidente. O documento é uma planta baixa para linhas de comunicação, funções, notificações necessárias e etapas a serem tomadas para responder a qualquer violação de segurança.

Embora cada incidente seja inteiramente único, um CSIRP flexível e bem construído permitirá que uma resposta seja formulada rapidamente ao identificar as pessoas principais que devem ser incluídas, suas funções e seus protocolos de comunicação. Com essa estrutura definida, as etapas necessárias podem então ser tomadas para endereçar a tecnologia por trás do incidente ocorrido.

8 Fazer uma política, não um plano

Lembre-se sempre que o "P" no CSIRP significa "Planos" e não "Política". Ocasionalmente, a IBM revisa um CSIRP que parece mais um documento de política do que um plano. Qual é a diferença? Um plano compreende etapas acionáveis e funções enquanto uma política declara diretrizes abrangentes a serem aplicadas dentro da organização. Quando um incidente ocorre, você realmente quer ficar lendo a política da empresa para formular um plano? É claro que não. Você gostaria de um plano bem definido que diga o que fazer.

9 Deixar de atribuir um proprietário e manter o plano atualizado

Seu CSIRP tem muito em comum com seu jardim. Ambos se desenvolvem com o tempo, exigem manutenção e atenção e devem ter proprietários responsáveis pelo seu bem estar. Ao definir um CSIRP, um proprietário deve ser atribuído ao documento. Isso significa que uma pessoa específica, não um departamento ou posição, seja responsável por manter o documento, garantindo que a equipe e os procedimentos contidos nele ainda sejam relevantes, além de coordenar o teste anual.

Sem um proprietário específico, o documento pode definhar, se tornar estagnado e possivelmente causar o aumento nos tempos de resposta a incidentes. Além disso, para ser eficiente, essa pessoa precisa ter o apoio executivo para a função de propriedade ou estar em uma posição alta o suficiente para alocar recursos para testes e atualizações.

Um CSIRP deve ser regularmente atualizado, ao menos duas vezes ao ano, além de ser atualizado após eventos significativos como a conclusão de uma fusão ou aquisição, grandes alterações de infraestrutura ou de pessoal, ou um incidente de segurança cibernética. Em média, ao trabalhar com clientes, vemos CSIRPs sendo atualizados a cada 18 a 24 meses – embora em nossa experiência, não seja incomum ver um CSIRP que não tenha sido atualizado em cinco anos. Na eventualidade de um incidente ocorrer, esse documento desatualizado é apresentado, desempoeirado e a equipe de resposta rapidamente descobre que a equipe principal nomeada no plano não está mais na empresa ou foram movidos para outras funções. O infeliz resultado final é um atraso na resposta – com consequências potencialmente significativas.

10 Ignorar o processo de fechamento do incidente

As lições mais valiosas de qualquer incidente podem ser aprendidas na revisão após a ação. Antes de um incidente ser oficialmente encerrado, a melhor prática é a realização de uma reunião de lições aprendidas, onde você pode avaliar a eficácia do CSIRP (funcionou bem?) e documentar a causa-raiz, bem como outras provas.

Mesmo que pareça que tudo correu como planeado durante um incidente, é provável que uma revisão pós-ação revele melhorias potenciais. Identificar erros ou questões que precisam ser alteradas só vai fortalecer o CSIRP e torná-lo mais capaz de atender às suas necessidades durante os incidentes futuros. Sua equipe de resposta pode estar ansiosa para deixar o passado para trás e retornar à operação normal, mas este último passo não deve ser negligenciado – muitas vezes é a parte mais importante do processo de resposta a incidentes.

Quão consistente é seu CSIRP?

A sua organização possui um Plano de Resposta a Incidentes de Segurança em Computadores (CSIRP) formal e documentado – e, em caso afirmativo, quando foi a última vez que seu CSIRP foi atualizado? Se suas respostas são diferentes de "sim" e "nos últimos seis meses", seria uma boa ideia falar com um especialista em segurança de TI de fora da sua empresa.

Na IBM, nós podemos ajudar os clientes a avaliar e melhorar um CSIRP existente ou ajudá-lo a construir um plano personalizado a partir do zero. Você pode começar com uma avaliação de alto nível para um investimento modesto e, com base em nossas conclusões e recomendações, decidir sobre seus próximos passos. Este trabalho é realizado pelos mesmos especialistas em segurança da equipe do Serviço de Resposta a Emergências da IBM, que trabalham lado a lado com os clientes durante situações reais de resposta a incidentes. Baseamos nossas melhores práticas CSIRP em padrões da indústria, como NIST (Instituto Nacional de Padrões e Tecnologia), ISACA (Associação de Auditoria e Controle de Sistemas de Informação), IETF (Força Tarefa de Engenharia de Internet) e ISO (Organização Internacional para Padronização).

Em caso de emergência, ligue para 1-888-241-9812

O Serviço de Resposta a Emergências da IBM (ERS) funciona 24 horas por dia, 7 dias por semana, 365 dias por ano, sendo composto por equipes de resposta a incidentes e especialistas em computação forense prontos para responder a incidentes de segurança no mundo todo. As Equipes de ERS estão acostumadas a lidar com ameaças à nossos clientes, tais como malware dia zero, intrusões de rede e outras ameaças de segurança avançadas.

Se você está enfrentando um problema de segurança grave e precisa de assistência imediata, ligue para a hotline da ERS em: 1-888-241-9812 ou +001-312-212-8034

Para mais informações

Para saber mais sobre como a IBM pode ajudar a proteger sua organização contra ameaças cibernéticas e reforçar a sua posição de segurança de TI, entre em contato com seu representante IBM ou Parceiro de Negócios IBM, visite o site: **ibm.com**/services/security

Para saber mais sobre a epidemia de violação de dados e o que você pode fazer para prevenir e responder a incidentes, visite o site: **ibm.com**/services/us/en/it-services/data-breach/index.html

Siga-nos no:

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produzido nos Estados Unidos da América
Janeiro de 2014

[1] IBM, *Serviços de Segurança IBM Índice de Inteligência de Segurança Cibernética*, Junho de 2013.

[2,3] Ponemon Institute, 2013, Estudo de Custo de Violação de Dados: Pesquisa de Referência e Análise Global patrocinada pela Symantec e realizada de forma independente pelo Ponemon Institute, maio de 2013.

Recicle