RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO – Um enfoque corporativo.

Ricardo Andrian Capozzi

São Paulo - SP - Brasil

RESUMO

O CERT Brasil define um incidente de segurança da informação como "qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores", ou seja, para haver um incidente não necessariamente deve ocorre corrupção dos dados.

Tal definição aglutina todas as situações em que uma entidade geradora de informação está em risco, como uma tentativa de invasão, desfiguração do portal, evasão de informações confidenciais, disseminação de malwares ou qualquer situação que comprometa os pilares da segurança da informação – Confidencialidade, Integridade e Disponibilidade. Assim, todo incidente deve ser tratado seguindo uma metodologia previamente definida pela instituição prevista e normalizada dento da Política de Segurança da informação e do Plano Diretor de Informática. Essa metodologia, conhecida como Resposta a Incidentes de Segurança, procura minimizar o impacto de uma ocorrência permitindo a normalização e restabelecimento dos sistemas o mais rápido possível.

Embutir na cultura organizacional que criar ou adotar um modelo e uma equipe de resposta a incidentes de segurança e de fundamental importância para diminuir prováveis danos, acelerando o tempo de reação preservando os ativos críticos da informação. Sua implantação não é uma tarefa simples, sobretudo em redes corporativas com ambientes heterogêneos.

Palavras Chave – Incidente. Segurança da Informação.

1. INTRODUÇÃO

Tornou-se primordial utilizar cada vez mais o meio público para troca rápida de informações em função da necessidade de acesso rápido, seja para efetuar processamento de transações, tomar decisões estratégias, executar pesquisas, entre outras demandas específicas.

A rede mundial, através de seus *links* intercontinentais, permite que em poucos segundos transações sejam efetuadas reduzindo o espaço geográfico através da aproximação virtual de fronteiras. Com a utilização da Internet, as empresas se estruturaram de forma a expor sua face para o mundo. E é justamente essa abertura e superexposição que faz com que a Internet, veículo de difusão de informações utilizado também para promover negócios, seja usada para finalidades obscuras como espionagem industrial, roubo de informações, chantagens e outros tipos de crimes cometidos contra o patrimônio dessas corporações. Por dizer, o contínuo crescimento e diversificação da Internet estão sendo acompanhado pelo aumento no número de incidentes de segurança.

Um site de comércio eletrônico não recebe somente visitas de consumidores interessados em adquirir seus produtos ou serviços. Muito se passa nos bastidores de um site transacional. Além da preocupação em prestar um bom atendimento, as empresas necessitam estar preparadas para visitantes hostis. As vezes, os *links* são inundados com tráfego de dados maliciosos: *portscans, exploits* e propagação de *worms* trabalham objetivando prejudicar ou fraudar a operacionalidade do site, gerando um problema de segurança.

2. OBJETIVO

Explanar e as principais características (técnico-gerencial) e etapas de uma abordagem metodológica para Resposta a Incidentes com a Segurança da Informação em ambientes corporativos.

3. MOTIVAÇÃO

As novas tecnologias de virtualização vêm carregadas de oportunidades e ameaças digitais. Esta realidade fomenta a pressão sobre os profissionais de Segurança da Informação, e direcionou os fabricantes de softwares de segurança na busca e desenvolvimento por soluções, exigindo novas estratégias para anteverem-se as vulnerabilidades preservando a operacionalidade de seus sistemas.

Tornar o ambiente de rede seguro é vital para a manutenção da estabilidade, produtividade, credibilidade e, principalmente, do faturamento. Tal necessidade pode ser saciada a partir da utilização correta de dispositivos e pela elaboração de politicas que possam governar o uso apropriado destes.

A preocupação das empresas está em blindar informações armazenadas ou que trafeguem dentro ou para fora de sua rede corporativa. A proteção da rede interna normalmente é baseada em definições de políticas que incluem

procedimentos de auditoria, métodos de autenticação, normas para utilização de Internet, correio eletrônico, anti-malwares, *firewall*, etc.

Quando tais "dispositivos-processos" falham, suas barreiras são transpostas, gerando incidentes com a segurança da informação, que precisam ser bloqueados, mapeados, entendidos e tratados a fim de mitigar problemas futuros.

4. DEFINIÇÃO

Segundo o dicionário Aurélio, **incidente** é:

> ***Evento não planejado que tem o potencial de levar a um acidente. Evento que deu origem a um acidente ou que tinha o potencial de levar a um acidente.***

O CERT define como incidente de segurança qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores. Normalmente encaixam-se nessa definição todas as situações em que uma entidade de informação está ameaçada. Em geral, toda situação onde uma entidade de informação está em risco e considerado um incidente de segurança. Exemplos:

1. Varredura de portas.
2. Tentativas de acessos não validos.
3. Injeção de Código SQL.
4. Divulgação de informações critica e confidenciais.
5. Propagação de Hoax, Spam, Malwares, Internal mail-list.
6. Aplicação ou atualização de patches sem homologação.
7. Captura de pacotes.

Tais incidentes implicam em sérios riscos para a imagem corporativa podendo causar um impacto significativo se não tratadas adequadamente e no devido tempo.

A gravidade de um incidente é medida diretamente proporcional com o impacto causado no processo de negócio. Por dizer, a indisposição de um *web commerce* pode trazer grandes prejuízos à empresa que o mantém, já que seus clientes ficarão impossibilitados de realizar compras; ou o vazamento de informações para uma empresa concorrente sobre o lançamento de um novo produto poderá retirar de uma empresa uma valiosa vantagem competitiva.

5. METODOLOGIA DO PROCESSO DE RESPOSTAS A INCIDENTES

Todo incidente de segurança deve ser tratado seguindo uma metodologia previamente prevista e definida. Essa metodologia, conhecida como Resposta a Incidentes de Segurança ou Plano de Resposta procura minimizar o impacto de um incidente e permitir o restabelecimento dos sistemas o mais rápido possível.

Resposta a Incidentes de segurança é definida como um conjunto de protocolos ou "uma metodologia organizada para gerir consequências de uma violação de segurança de informação", e deve ser resultado dos esforços de diferentes equipes organizacionais e não apenas de T.I., agregando níveis gerenciais e técnicos.

Por se tratar de uma nova disciplina pouco difundida, algumas empresas só aprendem a tratar seus incidentes de segurança após sofrerem tentativas de ataques ou serem efetivamente invadidas e comprometidas. A resposta mais adequada quando se trata de incidentes de segurança deve ser parte da diretiva de segurança e de suas estratégias de análises de riscos.

Obtêm-se diversos benefícios nas respostas aos incidentes de segurança: com garantir a aderência das políticas de segurança da informação adotadas e a realização de ações corretivas, detectivas e preventivas.

6. GRUPO DE RESPOSTA A INCIDENTES

Após uma perturbação dos sistemas computacionais, um evento é gerado e inicia-se um processo de tratamento ao incidente por uma equipe especializada. Este tratamento é um processo complexo e por vezes dispendioso, e é nominado como "pronta resposta de segurança".

Os CSIRT´S (*Computer Security Incident Response Team*), conhecidos especialistas em resposta a incidentes de segurança, são os formadores desta equipe por vezes heterogênea, acolhendo especialistas das áreas técnica e operacional. Esta equipe tem um papel fundamental na mitigação do número de incidentes, pois atuam diretamente em sua solução e tempo de resposta.

Assim, sua principal função é a de atualizar os alarmes de detecção e desenvolver um processo de tratamento de incidentes de segurança como a prontificação da resposta o mais célere o possível.

6.1 GESTÕES DE INCIDENTES DE SEGURANÇA

A equipe CSIRT´s deve estar apta a lidar com quaisquer tipos de incidentes de segurança dentro do ambiente coorporativo no que se refere às relações de T.I. Faz parte das principais atribuições desta equipe as seguintes funções:

- Verificar violações.
- Documentar e registrar os incidentes de segurança devidamente, preservando evidências.
- Realização de auditorias internas de sistemas de informação e de rede por meio de processos estruturados.

- Manter se atualizado sobre novas vulnerabilidades e estratégias sobre ataques submetidos pelos invasores para ampliar a base de conhecimento.

- Buscar e desenvolver novas tecnologias para diminuir as vulnerabilidades e riscos de segurança da informação.

- Prestação consultoria para área de segurança da informação.

- Utilizar como recurso e fonte de base de conhecimento a ISO/IEC 27001.

Para formação dos CISRT´s, é necessário haver:

- Treinamento adequado de acordo com o uso e localização de sistemas de segurança da informação, levando em consideração o uso de computadores portáteis com esses sistemas instalados para que haja uma resposta de incidentes mais rápidas e customizando o tempo de tratativa do mesmo.

- Disponibilizar informações de sistemas de emergência e, um local central, porém *offline*, sendo mais claro um servidor com informações, por exemplo: senhas de sistemas, endereços IP's, configurações de aplicativos, listagens de liberações de regras de *firewall,* contatos, procedimentos operacionais, entre outras coisas de suma importância para a área de segurança da informação – todos devidamente protegidos! Com isso todas as informações estarão disponíveis e devem ser mantidas com as devidas seguranças tanto físicas quanto lógicas.

7. AVALIAÇÕES DE SEGURANÇA

Há duas formas diretas de se agir na Segurança da Informação.

1ª Reativamente: Ação executada sempre após uma invasão ou pelo conhecimento de uma tentativa de invasão conhecida como ataque, entendendo seu *Modus Operandi* e criando um plano para mitigar as vulnerabilidades que não foram previstas e/ou monitoradas pela Análise de Risco. Esta abordagem atua em todas as camadas da empresa, e deve envolver as áreas de risco do incidente. A vantagem, se é que há uma, é que se corrige uma falha que foi descoberta e explorada por um terceiro – nem sempre com boas intenções.

2ª Proativamente: Neste caso a Análise e Avaliação dos Riscos dos ativos envolvidos em T.I. são fundamentais, para não dizer essenciais. Há vários métodos e metodologias, bem como uma ampla gama de ferramental disponível para se elaborar e previr a ponto de poder mitigar os problemas com segurança em que se pode aceitar e gerenciar os riscos inerentes ao negócio. É nesta ação que se enquadram os Testes de Intrusão executadas pelos especialistas em Segurança da Informação

Ambas as abordagens despendem recursos para serem elaboradas, aplicadas e mantidas, entretanto, por sua natureza preventiva, a segunda é

indiscutivelmente a que não afeta a imagem da empresa, por vezes incomensurável e irretratável.

Estas atitudes visão lacrar alguma possível lacuna (vulnerabilidade) técnica-operacional que possa ser explorara por uma atacante. Já quando todas as barreiras de segurança foram passadas ocorre um incidente que então ativa prontamente o processo de resposta. Aqui então se vê a lei da ação e reação em ação - sem trocadilhos!

8. CAMADAS DE CONTROLE EM SEGURANÇA DA INFORMAÇÃO

A maturidade de um sistema de segurança da informação no qual a base para obter uma resposta a incidentes é dada pele definição de políticas que irão reger as estratégia e procedimentos a serem adotados juntamente com os níveis hierárquicos acionados, e é dada pela seguinte estrutura.

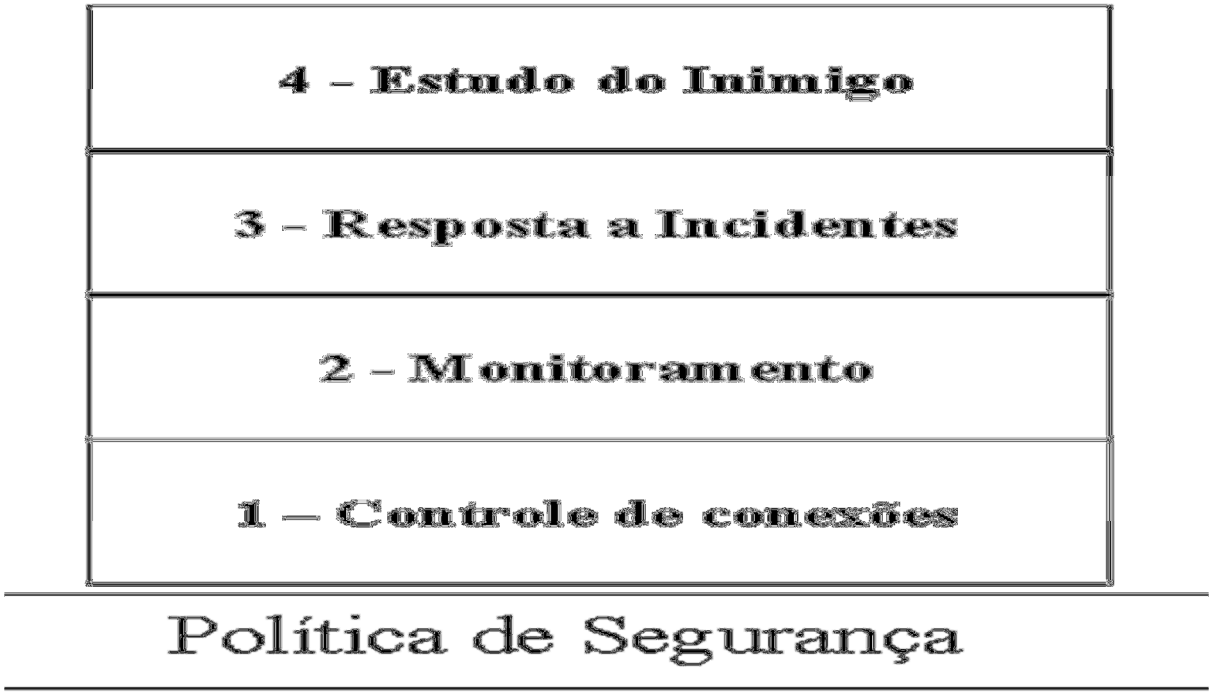

Figura 1 – Maturidade dos Sistemas de Segurança. ABSOLUTA (2002)

Melhor descritas:

Camada 1 - Controle de Conexões donde são inseridas barreiras com o intuito de conter as ameaças que podem ocasionar um incidente. Para tal, utilizam-se estruturas como *firewalls*, ACL, conexões de estados *statefull,* sistemas anti-vírus, etc.

Camada 2 - Observação e detecção de tentativas de intrusão via IDS/IDP que monitoram o tráfego da rede e *hosts* buscando padrões de ataque.

Camada 3 - Resposta a Incidentes com procedimentos de: identificação do incidente, notificação das pessoas responsáveis, coleta e preservação de evidências, rastreamento da origem, acionamento de contingências e ações de contra-resposta.

Camada 4 – Estudo do Inimigo, em que se procura analisar o atacante, buscando-se identificar as técnicas e táticas utilizadas ou seu Modus Operandis. Para isso, pode-se lançar mão de ambientes destinados a detectar atividades maliciosas, como as Honeynets. O objetivo deste estágio e o estudo das ações e motivação dos invasores com a finalidade de compreender sua mentalidade a fim de melhor proteger os sistemas críticos.

Este artigo focará o entendimento descritivo da terceira camada.

9. ETAPAS DE UM PLANO DE RESPOSTAS A INCIDENTES

A literatura específica fornece diretrizes para a criação de um plano de resposta a incidentes de segurança em ambientes corporativos. No entanto, a elaboração de um processo de tratamento de segurança passa por varias etapas que devem estar em conformidade com a política de segurança de cada instituição, que possuem idiossincrasias, e por ter que prevê-las atuantes em ambientes heterogêneo, o que aumenta consideravelmente sua complexidade.

Assim, para uma melhor ação do tempo de resposta, um processo estruturado faz-se necessário, e que deve contemplar:

- A diminuição de quantidade e gravidade de incidentes de segurança.
- A gestão de Incidentes de segurança.
- O plano de ações para respostas de incidentes de segurança.

9.1. REDUÇÃO DA QUANTIDADE E GRAVIDADE DE INCIDENTES DE SEGURANÇA.

Algumas abordagens na disciplina de Segurança da Informação têm natureza Preventiva e outras Corretivas. Em geral precisamos nos preparar para situações adversas e não previstas, pois é melhor sempre prevenir e estar preparado para o pior cenário. De qualquer forma, é impossível impedir todos os incidentes de segurança da informação. Mas ao ocorrer um incidente de segurança, será necessário trabalhar para que o impacto seja mitigado. Assim, os itens a serem seguidos referentes a esse tópico devem contemplar:

1- Garantir a aplicação de políticas e procedimentos de segurança em sua organização. Alguns incidentes são criados pelos desconhecimentos de políticas diretivas de segurança por não entenderem os processo e o que devem ser seguidos. Todos os procedimentos e diretivas de segurança

devem ser integralmente testados a fim de garantir o nível de segurança adequado.

2- Analisar regularmente o ambiente. As análises devem ser realizadas por um especialista da área de segurança da informação.

3- Validar todas as atualizações de sistemas. Por exemplo: Sistema operacional, antivírus e etc.. Garantindo que os mesmos estejam utilizando seus patches e vacinas atualizadas.

4- Estabelecer treinamentos para áreas de tecnologia da informação e usuários finais. Exibição de cartazes com informações de responsabilidades e restrições de usuários finais, para até mesmo para obtenção de evidências.

5- Verificar *logs* de sistemas regularmente para analisar e detectar intrusões, e da colocação de alarmes com regras restritivas previstas na politica de Segurança.

6- Avaliar e testar do processo de *Backup e Restore*, para iniciar prontamente o Plano de Recuperação de Desastre se necessário.

7- Observar os processos das atividades operacionais e garantir os três pilares da segurança da informação. Confidencialidade, Integridade e Disponibilidade.

Vale de orientação que os agentes da ameaça que ferem as políticas e diretivas de segurança da informação podem ser: funcionários, terceiros, visitantes, fornecedores, ou quem se menos esperar ou suspeita.

9.2. PLANO DE AÇÃO PARA RESPOSTAS DE INCIDENTES DE SEGURANÇA

No planejamento do plano de resposta a incidentes, não se deve questionar **SE** um incidente ocorrerá, mas sim, **QUANDO**, ou seja, sempre haverá oportunidades geradoras de incidentes de segurança ou vulnerabilidades, de maior ou menor grau de gravidade.

Portanto é necessário estar preparado para que seus impactos sejam os menores possíveis. Para tal efeito, estabelecem-se medidas pré e pós-incidente dentro do plano. As medidas pré-incidentes devem prever a:

- Definição detalhada dos procedimentos a serem adotados.
- Classificação dos recursos a serem protegidos.
- Implantação de mecanismos de segurança.
- Definição de equipe multidisciplinar para atuar em caso de incidentes.
- Classificação dos incidentes quanto ao nível de gravidade.
- Elaboração da estrutura administrativa de escalonamento do incidente.
- Montagem de um *kit* de ferramentas para atuar em incidentes em plataforma diversas, a exemplo do *MUFFIN.*

- Quem avisar no caso de incidentes.

9.3. ACIONAMENTO DO PLANO DE AÇÃO PARA RESPOSTAS DE INCIDENTES DE SEGURANÇA

Todos os colaboradores da área de T.I. devem atentar-se para a possibilidade de um incidente acontecer. A equipe responsável pela gestão dos incidentes de segurança deve receber as informações da ocorrência pela área de tecnologia da informação que no caso, é a responsável pela informação da ocorrência e coleta das devidas evidências de acordo com seu escopo de trabalho.

Caso haja alguma anormalidade ou algo suspeito, os usuários finais devem informar a área de tecnologia da informação e não diretamente ao grupo responsável pela gestão de incidentes. A área de TI capacitada realizará um filtro para entender o que de fato esta acontecendo e se houver a necessidade acionará o grupo de gestão de incidentes de segurança informando-os sobre a devida ocorrência.

Um roteiro sugerido para o acionamento deste plano por parte da área de T.I. aos CSIRT's, deve seguir aglutinar as seguintes fases:

- Acionamento da área de Tecnologia da Informação.
- Realizar a análise inicial do processo comprometido.
- Informar ao grupo responsável pela gestão de incidentes de segurança a ocorrência de um incidente.
- Analisar os danos e diminuir os riscos.
- Classificar o incidente pela gravidade do comprometimento.
- Estancar o ataque.
- Recuperação do ataque.
- Garantir as devidas proteções nas evidências geradas.
- Organização das documentações geradas com as ocorrências dos incidentes de segurança.
- Documentar os danos e os custos gerados com a ocorrência.
- Revisar as políticas de resposta aos incidentes e atualizações em geral.
- Reportar as autoridades legais, se necessário.

9.3.1. Área de Tecnologia da Informação.

Esta área é capacitada nas políticas e diretivas de segurança de sua organização para entender as ocorrências e repassar as informações para o grupo responsável – CSIRT´S. Esta analise prévia é necessária para não ocorrer enganos e inconvenientes com os envolvidos, ou frustações com falsos positivos e negligências com falsos negativos. Assim, haverá um time muito mais objetivo, focado e eficaz.

9.3.2. Realizar uma análise inicial do processo.

Diversas atividades em seu ambiente de trabalho poderiam indicar um possível ataque em sua organização. Um sistema de antivírus que esteja realizando uma manutenção preventiva em seu ambiente pode parecer que iniciar um processo de ataque ou algum software mal configurado poderá gerar ocorrências falsas positivas.

O mínimo requerido para uma avaliação inicial seria:

- A área de T.I. avaliar se realmente se trata de um incidente de segurança ou simplesmente um positivo falso. Ou seja, filtrar a informação antes de delega-la ou acionar o Plano de Resposta.

- Entender o incidente gerado identificando a gravidade. Analisar a informação realizando uma pesquisa mais profunda e posteriormente aceitar o dano, acionar a solução e minimizar o risco.

- Documentar todas as etapas do processo, pois serão utilizados quando um novo incidente de segurança for gerado.

9.3.3. Informar ao grupo responsável pela gestão de incidentes de segurança a ocorrência de um incidente.

Após a área de T.I. receber as informações de um suposto incidente de segurança de um usuário final e realizar as devidas analises descritas no item 9.3.2, a ocorrência deverá ser repassada ao grupo responsável pela gestão de incidentes (CSIRT´s). Esse grupo irá analisar a ocorrência e tomar as devidas providências iniciando o Plano de Resposta a Incidentes.

9.3.4. Analisar os danos e diminuir os riscos.

É necessário agir rapidamente parta diminuir os efeitos de um ataque. A resposta dependerá da organização e gravidade do ataque. Entretanto deve-se atentar em manter as seguintes premissas.

- Preservar a vida humana e segurança das pessoas.

- Proteger dados críticos, sigilosos e confidencias.

- Proteger software e hardware contra ataques ou bloqueios.
- Diminuir a interrupção dos recursos tecnológicos, ou negação de serviços - DoS.

9.3.5. Classificação do incidente pela gravidade do comprometimento.

O descritivo abaixo tem como finalidade guiar a empresa no entendimento das Violações mais comum.

Violação de segurança	Descrição
Falsidade	Alegada intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informatizados ou por qualquer outra forma interferir num tratamento informatizado de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem. Inclui a mistificação de sites Web para roubo de credenciais e a distribuição de mensagens de correio eletrônico de *phishing ou spam.*
Interferência	Alegada ação intencional e não autorizada ou a tentativa de impedir ou interromper gravemente o funcionamento do sistema informatizado, introduzindo, transmitindo, danificando, apagando, deteriorando, alterando, suprimindo ou tornando inacessível qualquer componente de software ou hardware. Inclui os ataques de negação de serviço – Dos, DDoS, DRDoS.
Acesso ilegítimo	Alegado acesso ou tentativa de acesso intencional e não autorizado à totalidade ou a parte do sistema informatizado. Inclui roubo de informação, nomeadamente segredo comercial, industrial ou dado confidenciais protegido por lei.
Interferência em dados	O ato intencional e não autorizado ou a tentativa de apagar, danificar, deteriorar, alterar, suprimir ou tornar inacessíveis dados do sistema informatizado. Inclui *malware* e sua distribuição por correio eletrônico.
Captura não autorizada	O ato intencional e não autorizado de reunir informação sobre tráfego de redes e sistemas informatizados.
Violação de direitos de autor	Alegada violação de direitos autorais, independentemente dos conteúdos serem constituídos por informação, código fonte, projetos gráficos ou quaisquer outros elementos do sistema informatizado protegido por direitos de autor.
Mensagem de correio eletrônico não solicitado	Recepção ou envio de mensagens de correio electrónico não solicitadas, quer sejam produzidas para efeitos de marketing direto ou sem motivação aparente. Não inclui distribuição de *malware* ou ataques de *phishing.*

Outras violações de segurança	Outras violações da política de segurança informática.

Fonte: http://www.cert.pt/index.php/component/content/article/21-institucional/participacao-de-incidentes/1525-classificacao-de-incidentes

9.3.6. Recuperação de um ataque.

Tratativa de recuperação de um ataque. Primeiramente identifica-se com que gravidade o sistema foi comprometido para entender o que está acontecendo e planejar sua contenção. Dessa forma há como realizar um planejamento de recuperação mais eficiente. Por exemplo: entender o ataque, como diminuir o risco, tempo de recuperação e tratativa do incidente de segurança. Citando algumas etapas:

- Identificar qual foi o sistema alvo.
- Identificar qual sistema foi comprometido.
- Identificar qual a classificação do incidente.
- Identificar a natureza e origem do ataque.
- Analisar a intenção do ataque.
- Verificar se algum sistema foi danificado ou alterado.
- Analisar os logs de aplicativos ou dados para verificar se algo foi acessado e garantir sua integridade e confidencialidade.

Realizando essas ações, ter-se-á uma resposta objetiva e realista do ambiente molestado.

Deve-se atente ao tempo de resposta ao incidente, pois o mesmo é essencial. Procedimentos mais rápidos devem ser realizados antes dos mais demorados, mitigando problemas com a imagem da organização.

Se necessário retornar as atividades desde um ponto de parada, os *backups* mais recentes ou até anteriores podem não ser suficiente para se obter um estado funcional antes do incidente. É um risco que precisa ser muito bem gerenciado!

9.3.7. Garantir as devidas proteções nas evidencias geradas.

Esta fase busca tomar as medidas legais cabíveis contra o intruso ou agente da causa do incidente. Nesse caso até mesmo para preservar essa opção a própria evidência gerada deverá ser utilizada. Se necessário mais informações, buscar referencial teórico na disciplina de Pericia Forense Computacional de como obter provas e evidências legais.

Uma recomendação: importante realizar as cópias de segurança dos sistemas, mesmo os comprometidos, sempre que necessário para gerar evidência legal. O *backup* é extremante importante em qualquer organização, não importa seu porte ou atuação mercadológica, e deverá ser armazenado em local protegido (para este referência consulte a ISO 2700).

Esses *backups,* tanto de sistemas e evidências podem ser utilizados em caso de contramedidas a ataques e também para garantir a disponibilidade e integridade da informação. Em outros casos o beneficio de manter a rotina de *backup* é garantir o tempo de resposta de, por exemplo, uma interrupção de funcionamento de um sistema que tenha sido apagado por engano, assim o tempo de restauração é muito menor do que a correção do sistema.

Por fim, é fundamental realizar cópias dos *logs* de todos os sistemas e suas rotinas mantendo-os por mais de 365 dias.

9.3.8. Organização das documentações geradas com ocorrências dos incidentes de segurança.

Os CSIRT´s, grupo responsável pela gestão de incidentes de segurança deve manter documentado todo o processo referente a qualquer incidente, gerando um histórico ou base de conhecimento para consultas futuras. Isso deve incluir uma descrição detalhada da ocorrência como: data, hora, pessoas envolvidas, ações corretivas, preventivas, ações tomadas e coleta de evidências.

Posteriormente, essa documentação será tratada, registrada, assinada e revisada pelos responsáveis legais. Também é necessário proteger essas informações/evidências conforme citado anteriormente preservando-as por um período não menor do que cinco anos. Uma documentação robusta oferece fundamentos para tomada de devidas providências em caos de acionamento do plano de resposta.

Por fim, monitorar e documentar incidentes, suportarão a equipe gerar indicadores e métricas que ajudarão numa visão mais ampla do processo e menor tempo de respostas dos próximos incidentes.

9.3.9. Documentar danos e custos gerados com a ocorrência.

Ao identificar um determinado dano, deve-se ter ciência dos custos diretos e indiretos relativos ao incidente analisado. Os custos e danos gerados serão evidências importantes caso opte-se por executar qualquer ação legal. Nesta etapa busca-se coletar custos gerados com:

- Perda de informações proprietárias ou confidencias.
- Tempo dos profissionais para analisar as violações.
- Softwares de análise e recuperação de dados.

- Possíveis multas por de tempo de indisponibilidade de ambiente gerado por ataques.

- Reparo e possibilidade de atualização de medidas de segurança física.

- Danos que podem interferir na continuidade dos negócios da organização.

Como dito no item 9.3.7, a Forense Computacional ajudará a empresa capturar tais evidências preservando as prerrogativas legais.

9.3.10. Revisar as políticas de resposta aos incidentes e atualizações em geral.

Processo final extremamente importante, que examina todos os procedimentos adotados para mitigar ou tratar incidentes. Há várias metodologias para atualização e adequação das politicas que preveem os planos de resposta incidentes.

Um questionário focado pode ser o da revisão das etapas do processo para identificar pontos fortes e fracos sugerindo melhorias e modificações dos processos. Isto auxiliará a tratativa dos próximos incidentes de seguranças que podem ocorrer quando se ferir as políticas de segurança da informação em sua organização.

10. PROJETO MUFFIN

Trata-se de um projeto de elaboração de uma lista de ferramentas para resposta a incidente, ou seja, é um *Incident Response Toolkit*, que suporta a criação de *pendrives* com ferramental que ajuda na coleta de informações voláteis para posterior análise dos eventos.

O projeto engloba 3 módulos:

1- O Pen MUFFIN. Que é um toolkit.
2- O MUFFIN Baker, uma ferramenta que permite configurar e gerar o Pen MUFFIN.
3- O MUFFIN Report, que acessa os dados gerados/coletados pelo Pen MUFFIN.

Detalhes de como obter e usar esta caixa de soluções veja referência MUFFIN

11. CONCLUSÃO

Um incidente poderia corromper potencialmente os dados por muitos meses antes da descoberta. Portanto, é importante que como parte do processo de resposta a incidentes, se determine a duração do incidente.

Ao criar um modelo de gestão de resposta de incidentes de segurança, a empresa deve basear-se nos pilares da segurança da informação, atuando desde a

comunicação de um incidente pela área de T.I., no qual já realizou um filtro para identificar se realmente há um incidente a ser tratado; e, realizando as etapas do processo descrito na politica, aceitando o incidente, iniciando o plano de resposta e posteriormente como tratá-lo buscando o mínimo impacto para a imagem da empresa.

Vale ressaltar que o profissional da área deve sempre se manter atualizado, pois os processos e politicas do plano gestor de incidentes poderão sofrer mudanças repentinas e não previstas.

A última parte do Plano de Resposta a Incidentes de segurança consiste em avaliar todo o processo de tratamento de incidentes e verificar a eficácia das soluções implantadas pelo tempo de resposta. As lições aprendidas durante todo o processo devem ser documentadas e propagadas, descrevendo formas de obter melhores resultados.

Por fim, discutir tal procedimento para gerar uma metodologia ampla desde a parte processual como identificação do incidente, taxonomia, e procedimentos de tratativas do evento, etc. faz parte do novo cenário da área de segurança e do papel do C.S.O. com os CSIRT´s. Empresas que não tem um CSIRT´s deveriam pensar a respeito, pois nunca se sabe quando ocorrerá um incidente de segurança. Mas é certo que irá ocorre!

REFERÊNCIAS BIBLIOGRÁFICAS

ABSOLUTA**. Resposta a Incidentes de Segurança.** http://www.absoluta.org/seguranca/seg_resposta_incidente_1.htm>. 2002.

AUGUSTO, Pedro**. Introdução aos honeypots**. http://www.dicas-l.com.br/dicas-l/20070321.php. 2007.

BROWN, Moira J. West et al**. Handbook for Computer Security Incident Response Team**. http://www.sei.cmu.edu/publications/documents/03.reports/03hb002.html. 2003.

CERT.pt. **Política de classificação de incidentes do CERT.PT**. http://www.cert.pt/index.php/component/content/article/21-institucional/participacao-de-incidentes/1525-classificacao-de-incidentes. 2013.

CERT.br. **Cartilha de Segurança para Internet.** http://www.cert.br/cartilha. 2013.

CERT/CC. **Computer Security Incident Response Team FAQ.** http://www.cert.org/csirts/csirt-faq.html. 2013.

CERON, João, et al. **O processo de tratamento de incidentes de segurança da UFRGS.** TRI - Time de Resposta a Incidentes de Segurança da Universidade Federal do Rio Grande do Sul Centro de Processamento de Dados. RS. 2010.

GUIMARÃES, Célio Cardoso et al. **Forense Computacional: Aspectos Legais e Padronização.** http://www.las.ic.unicamp.br/paulo/papers/2001-WSeg-flavio.oliveira-marcelo.reis-forense.pdf. 2001.

Kenneth R. Wyk, R. F.. **Incident Response.** O'Reilly & Associates., Sebastopol, California, USA. 2001

MANDIA, Kevin. PROSISE, Chris. **Incident Response. Investigation Computer Crime**. Osborne. 2002.

MICROSOFT TECHNET. **Incident Response Class**. http://technet.microsoft.com/pt-br. 2013

MUFFIN, Projeto. **Muffin - Master Unit For Forensics Investigation**. Rodrigues, Tony. Nakano, Vitor. 2013.

RESUMO CURRICULAR

Ricardo Andrian Capozzi possui graduação em Tecnologia da Informação pela Faculdade de Informática e Administração de São Paulo e pós-graduação nas áreas de Análise de Sistemas, Segurança da Informação, Marketing Internacional, Gestão de Negócios, Didática Superior em Tecnologia e Engenharia da Computação. Professor da FATEC - FACULDADE DE TECNOLOGIA DE SÃO PAULO, Faculdade Mauá e Faculdade Carlos Drummond de Andrade para graduação e pós-graduação. Atua como consultor de bancos e plataformas eletrônicas para o Banco Citibank S.A., com experiência na área de Ciência da Computação enfatizando Segurança da Informação e Redes. Contato: 11-98280-3133 – rackster@ig.com.br