Curso de Tecnologia em Redes de Computadores
Disciplina: Auditoria e Análise de Segurança da Informação - 4º período
Professor: José Maurício S. Pinheiro

AULA 3: Resposta a Incidentes de Segurança

A tecnologia da informação é um componente vital e cada vez maior da vida moderna. No entanto, a mesma tecnologia que permite que as pessoas acessem, gerenciem e compartilhem informações instantaneamente pode ser usada de forma indevida por indivíduos e empresas para invadir a privacidade alheia.

As organizações investem em segurança da informação por necessidade de sigilo, confidencialidade e combate ao vazamento de informações, a fraudes e diminuição de erros e acidentes. Em grande parte, a investigação e a perícia técnica tem contribuído para melhorar os níveis de segurança nas redes de comunicação. Entretanto, a dificuldade no levantamento das evidências, requer metodologias especificas, necessitando de conhecimento técnico e jurídico para emitir laudo consubstanciado para que a justiça possa enquadrar os delitos, como também um corpo técnico altamente qualificado.

Incidentes de Segurança

Mesmo tomando-se todas as medidas necessárias, falhas de segurança podem ocorrer, uma vez que alguma vulnerabilidade ainda não divulgada pode ser explorada ou um novo tipo de ataque pode ser utilizado. Dessa forma, não há como afirmar que um dado aparato de segurança está isento de falhas. Isto se deve principalmente ao fato de que tais aparatos, bem como os serviços oferecidos através da Internet, são compostos por diferentes tipos de software, que por sua vez, possuem milhares de linhas de código que não estão imunes a erros de programação. Outro ponto que deve ser considerado é que aproximadamente 70% dos incidentes de segurança possuem origem no interior das organizações. Desta forma, mesmo que a Internet não faça parte de nenhuma etapa dos processos produtivos da instituição, teoricamente ela não está livre de ser vítima de um incidente desse tipo.

Segurança, em geral, pode ser alcançada através da prevenção, preensão, inibição, desvio, bem como, detecção de ataques e contramedidas de proteção e eliminação de intrusão. Considerando que não há esquema de segurança imune a falhas, torna-se então necessária a definição de procedimentos a serem adotados no caso de um ataque bem sucedido, além da presença de pessoal capaz de executar tal função. A preparação para a resposta a um incidente de segurança deve começar bem antes do evento propriamente dito, sendo necessária a existência de uma estrutura previamente elaborada para que o acontecimento possa ser tratado com a rapidez e confiabilidade necessárias.

O primeiro aspecto a ser considerado é o cuidado com a configuração e monitoramento (políticas de auditoria) de todos os hosts que compõem a rede, uma vez que os incidentes podem possuir desdobramentos totalmente imprevisíveis em virtude do desconhecimento dos objetivos e do nível técnico dos agentes causadores. A tomada de medidas preventivas durante a configuração e a instalação de programas apropriados pode minimizar a imprevisibilidade das conseqüências das ações do atacante. Tais medidas têm como objetivo ampliar os vestígios das operações ilegais

que porventura possam ser executadas em uma determinada máquina, tornando assim uma posterior análise bem mais fácil de ser efetuada.

Dentre as medidas pode-se citar:

- Configuração adequada das políticas de auditoria;
- Utilização de ferramentas que garantam a integridade dos arquivos de sistema;
- Configuração das listas e controles de acesso aos sistemas.

Além da correta configuração de todo o parque de máquinas, a preparação para uma resposta a um incidente pode contemplar uma série de medidas que vão além de parâmetros técnicos de instalação e configuração do sistema operacional. Deve-se considerar, por exemplo, a elaboração de uma política de utilização dos recursos de Tecnologia da Informação que contemple a possibilidade de uma investigação, abordando assim questões como a quebra de privacidade e monitoramento de atividades. A definição de tal política requer debate entre todos os usuários e discussão da filosofia da organização, o que por muitas vezes não é uma tarefa fácil.

Outro aspecto a ser considerado é o fato de que durante uma auditoria de segurança não há tempo hábil para que se faça testes ou experiências, já que a pressão para que as atividades retomem a sua normalidade é grande. A melhor maneira de se obter a rapidez necessária é através da execução de procedimentos padrões previamente testados por pessoal qualificado. Um time de resposta a incidentes (TR) será a entidade responsável por coordenar as atividades antes, durante e depois do incidente de segurança. Apesar de ainda ser muito raro dentro das organizações, esse personagem é de extrema importância para o bom andamento das contramedidas a serem adotadas.

O time de resposta pode ser formado por uma ou mais pessoas com conhecimentos na área de segurança e deve assumir várias responsabilidades, dentre elas:

- Participar da elaboração da política de segurança determinando as ações que possam ser tomadas durante a remediação do incidente;
- Elaborar procedimentos de emergência a serem adotados durante os eventos;
- Preparar simulações de incidentes;
- Coordenar as atividades no caso de um incidente real.

Conhecer os ataques mais comuns, seguir o rastro dos atacantes, coletar evidências para comprovar fraudes, estudar as medidas legais para identificação de criminosos em meios eletrônicos são fundamentais. Além de, utilizar ferramentas de perícia digital como apoio para prova jurídica, e conhecer os limites jurídicos para a investigação também são atribuições dos profissionais participantes do TR.

Outro ponto a ser abordado pelo TR é a identificação das prioridades da organização. Do ponto de vista corporativo, um bom tratamento dado a um incidente é aquele que ameniza o impacto nos negócios. Os procedimentos devem considerar as prioridades da empresa, bem como saber identificar dentre os possíveis danos quais seriam mais prejudiciais à organização. São exemplos:

- Comprometimento da reputação da empresa, por exemplo, através da desfiguração de páginas web;
- Roubo de propriedade intelectual, por exemplo, espionagem industrial;
- Modificação ou destruição dos bancos de dados da organização.

Tal identificação serve também para amenizar o choque de objetivos entre o TR, que naturalmente busca remediar o acesso ilegal de forma concomitante à identificação e neutralização do agente causador do incidente, e a empresa que deseja o retorno à normalidade dos negócios o mais rápido possível.

Programa de Resposta a Incidentes

Tantos ataques internos como os ataques externos possuem padrões bem definidos, com uma seqüência de eventos que permitem estabelecer perfis ou modelos de comportamento. A ausência de monitoração e inspeção desses padrões nos computadores e redes ocasiona uma proliferação de ataques, sendo que não haverá uma reação rápida por parte dos administradores do sistema ou a geração e inspeção regular de registros de auditoria, tais como *logs* que possam determinar evidências.

Atualmente, existe uma forte tendência por parte das organizações em terceirizar funções de TI (outsourcing), inclusive funções relacionadas à segurança da informação em que geralmente incluem-se funções ligadas ao tratamento de incidentes. A vantagem de se terceirizar a manipulação de incidentes (TR Externo) decorre do custo de se manter pessoal capacitado, enquanto a contratação de uma empresa especializada geraria custo na medida em que houvesse demanda de seus serviços (Tabela 1). No entanto, um Time de Resposta interno (TR Interno) é dedicado àquela instituição e pode ser acionado rapidamente para enfrentar todos os problemas de rotina da organização, o que não acontece no caso de um terceiro.

Os programas de resposta a incidentes mais consistentes são os que possuem um TR interno robusto, dotado de considerável conhecimento técnico, em associação a um ou mais times externos para o caso de haver demanda de debates técnicos ou mesmo de pessoal. Esta pode ser uma solução extremamente eficaz e ainda assim manter os custos dentro de um limite razoável.

Tabela 1 – Comparativo de tipos de TR Externos

Tipo	Qualidades	Deficiências
Públicos	Baixo custo para organização. Boa fonte de estatísticas. Distribuição de alertas variados.	Não pode fornecer atendimento personalizado para cada organização.
Comerciais	Profissionais altamente especializados. Pagamento por demanda.	Desconhecimento da organização interna das instituições. Os problemas diários ainda devem ser manipulados internamente. O tempo para que uma equipe esteja fisicamente no local do incidente pode não ser constante.
SO	Atenções voltadas para a rápida solução das vulnerabilidades encontradas em seus produtos. Contam com a presença de projetistas e programadores dos produtos para resolverem os possíveis problemas.	Foco limitado. Ações podem ser influenciadas por leis de mercado.
Ad Hoc	Usado como último recurso, mas é melhor que a tomada de contramedidas com pessoal não capacitado ou ainda a não tomada de ação alguma. Podem instruir os membros da corporação, sobre as vantagens de se possuir um programa de resposta a incidentes.	Não há vínculos sólidos com a instituição.

Definição de Procedimentos

A elaboração e documentação dos procedimentos a serem executados durante um incidente de segurança, inclusive referentes à investigação das máquinas afetadas, são essenciais para a credibilidade e rapidez da resposta.

O TR deve possuir um conjunto de ações pré-definidas mesmo que estas não abordem todas as possíveis situações, uma vez que tal abrangência é difícil de ser conseguida em virtude da quantidade de imprevistos que podem ocorrer. Tais procedimentos são definidos como SOP's (Standard Operating Procedures). Basicamente estes documentos descrevem como o TR vai prover os serviços de que é encarregado.

Um aspecto importante a ser levado em consideração durante a elaboração dos SOP's é a atribuição de responsabilidades. Os procedimentos devem considerar aspectos da hierarquia da organização principalmente no que se refere à tomada de decisões, como o contato com TR ou indivíduos externos, além de instituir uma hierarquia de cargos e responsabilidades dentro do próprio TR:

- Quem será responsável pela manipulação das possíveis evidências;
- Quem deve fazer a notificação do ocorrido para outros setores da organização;
- Outros.

Exemplo de SOP

O contexto do presente SOP é o da análise *postmortem* de uma máquina vítima de um incidente de segurança. Após o desligamento da máquina em questão existe a necessidade de se efetuar cópias bit-a-bit de seu disco rígido para que os procedimentos de análise não sejam conduzidos a partir das evidências originais, evitando-se, assim, o risco de que um eventual erro do examinador venha a danificar ou alterar a evidência original de alguma forma.

Convém salientar que a ausência do conjunto de ferramentas condizente com os procedimentos propostos nos SOP's que abordam aspectos técnicos, pode decretar um atraso na resposta, o que conseqüentemente pode resultar em um aumento da extensão dos danos.

Caso o TR espere até que uma invasão ou qualquer outro incidente ocorra para identificar e instalar as ferramentas necessárias, não será possível agrupar versões funcionais das peças de software necessárias e nem adquirir o conhecimento necessário para utilizá-las corretamente em tempo hábil, fazendo com que os resultados fornecidos sejam mal interpretados ou imprecisos, inviabilizando uma análise consistente.

Tais ferramentas abrangem:

- **Ferramentas para captura de dados e configurações:** para se efetuar tal tarefa é necessário selecionar ferramentas próprias para análise forense, isto é, que se preocupem em preservar o estado original das evidências, não alterando, portanto, tempos de acesso ou qualquer outra informação que venha a deturpar o ambiente;
- **Programas para cópias de segurança:** com o intuito de preservar a "cena do crime" é interessante que se evite efetuar qualquer tipo de análise sobre as evidências originais (por exemplo, disco rígido), sendo assim recomendável a criação de cópias idênticas para que a partir delas sejam aplicados os devidos procedimentos. No entanto deve ser dada preferência para ferramentas que preservem todos os atributos originais, inclusive espaços vazios. No caso de um disco o ideal é que seja utilizada uma ferramenta para criação de imagens, que efetua cópias bit a bit das mais variadas origens;
- **Ferramentas para cálculo de hashes criptográficos:** devem ser utilizadas para garantir a integridade das evidências e dos programas utilizados durante a análise; desta forma é possível provar que não houve qualquer tipo de alteração maliciosa, seja das ferramentas, seja das evidências. Deve-se tomar muito cuidado com o armazenamento dos hashes a fim de se evitar qualquer tipo de fraude.

Descrição: Procedimento para duplicação bit-a-bit de disco rígido IDE proveniente de máquina envolvida em incidente de segurança.

Requisitos: Máquina confiável com quantidade de espaço livre em disco superior à capacidade total de armazenamento do disco que se deseja duplicar e programas originais para auditoria. Para que o TR seja capaz de fazer a coleta e manipulação das

possíveis evidências durante a resposta, é necessário ter instalado um grupo de ferramentas que irão auxiliar nesta tarefa.

Procedimento:

1. Documentar todas as informações relevantes impressas na superfície externa do disco, tais como modelo, fabricante, quantidade de cilindros e cabeças de leitura, além do registro das posições dos jumpers presentes no equipamento;
2. Instalar o disco na estação forense, no canal secundário e, para que não ocorram conflitos em relação às configurações de dominância (master/slave), o disco deve ser o único dispositivo presente no canal. Para os próximos passos será suposto o mapeamento do disco alvo;
3. Ligar a estação e executar a detecção de discos presente na BIOS, tomando o cuidado de documentar a geometria do disco detectado;
4. Identificar e documentar as partições presentes no dispositivo;
5. Calcular o hash MD5 de todos os dados contidos no disco;
6. Efetuar a cópia de cada bit presente no dispositivo analisado, incluindo os espaços aparentemente vazios. Notar que tal procedimento pode exigir uma considerável capacidade de disco da estação forense;
7. Calcular o hash MD5 do arquivo gerado no passo 6;
8. Verificar se os hashes criptográficos gerados nos passos 5 e 7 correspondem exatamente ao mesmo valor.

Deve-se atentar para o fato de que, quando uma máquina é identificada como alvo de um ataque ou suspeita de uso ilegal por parte de algum agente interno, não é seguro utilizar qualquer tipo de software ou biblioteca presente na máquina. Uma solução muito adotada é a cópia em CD de todos os programas necessários, especializados ou nativos, para neutralizar a tentativa de ocultar informações através da utilização de bibliotecas ou comandos adulterados.

Outro ponto a ser considerado é a existência de infra-estrutura para a análise, o que pode tratar-se apenas de uma máquina com uma grande capacidade de disco onde possam ser copiadas as imagens e os dados das máquinas a serem analisadas e onde programas e outros sistemas encontrados possam ser analisados com segurança.

Procedimentos Pós-incidentes

Existem inúmeros procedimentos sendo discutidos e utilizados internacionalmente, entretanto não é possível estabelecer um conjunto de medidas a serem adotadas por todas as organizações. Dentre os procedimentos mais importantes pode-se citar:

- **Documentação das ações tomadas:** todas as ações e decisões tomadas durante a abordagem da máquina vítima devem ser documentadas, sem exceção. O rigor na documentação do processo permite uma futura avaliação da resposta;
- **Coleta de informações voláteis:** utilizando o CD de ferramentas previamente criado devem-se executar os programas necessários para se coletar o maior número de informações voláteis possível, uma vez que só haverá uma chance de fazê-lo. As evidências colhidas devem ser armazenadas de maneira segura;

- **Desligamento da máquina:** O desligamento da máquina vítima deve ser feito de forma não convencional para se evitar a possibilidade de execução de algum programa destrutivo;
- **Cópia dos discos:** A coleta preliminar de informações (live analysis) na maioria das vezes não é suficiente para a solução do evento; por isso deve ser seguida de uma análise posterior minuciosa. Os discos devem ser copiados bit a bit e seus hashes armazenados, para que:
    - Os discos da máquina possam ser liberados, se for o caso;
    - A análise *postmortem* possa ser feita sobre cópias, garantindo que um erro não venha a comprometer o disco original.

Análise Forense

Embora as organizações se preocupem em utilizar mecanismos para aumentar a segurança dos sistemas que utilizam a rede de computadores, não há garantias de que elas não poderão ser vítimas de um incidente de segurança, mesmo que sigam todas as recomendações e implantem as mais modernas tecnologias.

No caso de uma ocorrência de incidente de segurança a organização deve agir da melhor maneira possível para evitar o agravamento da situação. Para isso existem os programas de resposta a incidentes, nos quais estão incluídas as metodologias de análise forense, e que, ainda hoje, são raros na maioria das organizações. A preparação para a resposta a um incidente de segurança passa pela elaboração de procedimentos e pela tomada de medidas que possam futuramente auxiliar a realização de uma investigação forense.

Forense Computacional

A forma como o TR executa seus procedimentos e investigações durante a resposta a incidentes, pode ter implicações durante uma futura ação judicial contra um atacante. Caso o TR opte por efetuar todo o processo de análise, com o intuito de responder às perguntas supracitadas, todos os procedimentos adotados por ele devem ser rigorosamente documentados e todas as medidas para a garantia da integridade das informações devem ser tomadas, pois de outra forma as informações obtidas não poderão ser utilizadas em um tribunal, ou seja, se o TR não conseguir comprovar a autenticidade dos resultados obtidos durante a análise forense, todo o processo legal pode ser comprometido.

Assim a investigação técnica em busca da solução de um crime pode estar fora da alçada do TR, dependendo da gravidade do incidente, do conhecimento e disponibilidade de seus componentes. Cabe ao próprio TR julgar se a resolução de determinado caso está dentro de sua capacidade ou se será necessário acionar uma terceira entidade, como a Polícia Federal, por exemplo.

A ciência forense é aquela exercida em favor da lei para uma justa resolução de um conflito. Em outras palavras, é aquela que se baseia em procedimentos científicos para a obtenção de informações que possam ser úteis durante uma disputa judicial. A forense computacional pode ser definida como a ciência de adquirir, preservar, recuperar e exibir dados que foram eletronicamente processados e armazenados digitalmente.

A forense computacional visa principalmente vistoriar e analisar todos os componentes físicos e os dados que foram processados eletronicamente e armazenados em mídias computacionais. Esta análise compreende a aquisição,

preservação, identificação, extração, restauração e documentação de evidências computacionais seguindo alguns princípios básicos que são comuns às análises de qualquer plataforma computacional e que foram originalmente herdados de bases da ciência forense.

O processo de análise no meio computacional é metódico e deve seguir procedimentos previamente testados e aceitos pela comunidade científica internacional, de forma que todos os resultados obtidos durante uma análise sejam passíveis de reprodução. Isto implica em utilizar uma metodologia padrão que provê proteção às evidências através da definição de passos comuns que devem ser seguidos durante o processo de investigação. Caso os procedimentos utilizados na manipulação das evidências sigam todas as recomendações previstas nos padrões, não há como contestar sua integridade, fazendo com que possam ser utilizadas como prova em um julgamento.

A perícia em um computador suspeito de invasão ou mesmo um computador apreendido em alguma batida policial envolve uma série de conhecimentos técnicos e a utilização de ferramentas adequadas para análise. Existe a necessidade de se conhecer minúcias do sistema operacional para que se tenha uma noção global de todos os efeitos das ações do perito. Quanto à necessidade de se utilizar ferramentas específicas para análise, esta decorre da obrigatoriedade de não se perturbar o sistema que está sendo analisado (perturbações essas que podem ser traduzidas como mudanças nos tempos de acesso aos arquivos). Ferramentas convencionais não têm a preocupação de manter a integridade dos tempos de acesso.

Apesar do consenso em torno da necessidade de padronização, a definição de procedimentos para a forense computacional encontra dificuldades, uma vez que existem dezenas de tipos de mídia, sistemas operacionais com inúmeras versões, diferentes tipos de hardware e arquitetura. Além disso, o fato de que cada caso possui circunstâncias praticamente únicas, dificulta a definição de procedimentos que cubram todos os possíveis aspectos de uma análise.

Perícia Forense Computacional

O profissional da computação forense executa os serviços de investigação, rastreamento, recuperação de dados, laudos periciais e consultoria, através do conhecimento especializado e a utilização de técnicas e métodos que levem ao diagnóstico e o resultado, sempre submetido ao princípio da confidencialidade. Ele utiliza de métodos científicos para preservar, coletar, restaurar, identificar, documentar e apresentar as evidências digitais - capazes de determinar, por exemplo, se um sistema computacional sofreu uma violação.

A preocupação investigativa e a necessidade de produzir um relatório com as questões que evidenciam os crimes computacionais exigem que peritos ou especialistas, além de entender do código penal e civil, saibam como proceder tecnicamente com exames de hardware e software. Um importante aspecto a ser ressaltado na análise forense computacional é a documentação rigorosa de todas as ações tomadas pelo examinador durante a análise. Devido ao stress causado por um incidente de segurança, muitas vezes a documentação das decisões e ações não são devidamente efetuadas, o que pode prejudicar uma futura ação judicial contra os responsáveis, pois pode inviabilizar uma avaliação do tratamento dado às evidências.

A coleta de informações para análise (*information gathering*) é uma importante metodologia para a perícia forense de um sistema computacional invadido, buscando a extração de evidências nas informações coletadas e correlação dessas evidências encontradas. Além da correta documentação, pode-se citar mais alguns princípios das

demais disciplinas forenses, herdados pelo meio computacional, para os procedimentos de perícia forense computacional:

- **Réplicas:** efetuar as análises sempre sobre cópias idênticas das evidências originais, evitando-se que um erro do examinador venha a comprometer as informações, inviabilizando a realização de um novo exame para a validação dos resultados alcançados;
- **Garantia de Integridade:** existência de procedimentos que visem garantir a integridade das evidências coletadas. No mundo virtual a autenticidade e a integridade de uma evidência podem ser verificadas através da utilização de algoritmos de *hash* criptográfico como o MD5, SHA-1 e o SHA-2. Além disso, é possível armazená-las em mídias para somente leitura, como CD-ROM;
- **Ferramentas Confiáveis:** não há como garantir a confiabilidade dos resultados obtidos durante uma análise se os programas utilizados não forem comprovadamente idôneos.