O processo de tratamento de incidentes de segurança da UFRGS

João Ceron, Arthur Boos Jr, Caciano Machado, Fernanda Martins, Leandro Rey

[1] TRI - Time de Resposta a Incidentes de Segurança da
Universidade Federal do Rio Grande do Sul
Centro de Processamento de Dados
Rua Ramiro Barcelos, 2574 – Portão K – Porto Alegre – RS

{ceron,boos,caciano,flmmartins,leandro}@cpd.ufrgs.br

Resumo. *O processo de resposta a incidentes de segurança tem fundamental importância para diminuir os danos causados por ataques. A implementação de um processo de resposta a incidentes não é uma tarefa simples, sobretudo em instituições de ensino que constituem um ambiente bastante heterogêneo. Este trabalho busca discutir o processo de resposta a incidentes em instituições de ensino, apresentando exemplos práticos de como um processo consistente pode ser implementado.*

1. Introdução

O contínuo crescimento e diversificação da Internet está sendo acompanhado pelo aumento no número de incidentes de segurança [CERT.br b]. A devida resposta aos incidentes de segurança é um processo complexo e dispendioso para as equipes de segurança da informação.

Os times de resposta a incidentes de segurança (CSIRTs) tem um papel fundamental na diminuição do número de incidentes, pois atuam diretamente na solução e detecção dos problemas de segurança. Para uma maior eficiência, os CSIRTs devem constantemente atualizar seus meios de detecção e, sobretudo, desenvolver um sólido processo de tratamento de incidentes de segurança [FIRST]. A literatura fornece diretrizes para a resposta a incidentes de segurança. No entanto, a elaboração de um processo de tratamento de segurança passa por várias etapas que devem estar atreladas à política de segurança de cada instituição. As instituições de ensino possuem características peculiares pois cada unidade possui demandas específicas o que torna o ambiente bastante heterogêneo e aumenta consideravelmente a complexidade do processo de resposta a incidentes de segurança.

Diante disso, este trabalho tem por objetivo discutir e apresentar exemplos do processo de resposta a incidentes de segurança numa instituição de ensino. Acredita-se que a discussão do processo, tendo como base a implementação prática realizada na Universidade Federal do Rio Grande do Sul, pode contribuir na implementação ou revisão do processo em outras instituições de ensino.

Este trabalho está estruturado na seguinte forma: na primeira seção, é apresentada a introdução e motivação do trabalho; na segunda, os incidentes de segurança são caracterizados; na terceira, é apresentado o processo de resposta a incidentes de segurança; na

quarta seção, como foi realizada a implementação do processo na UFRGS; as conclusões encerram o trabalho.

2. Incidentes de Segurança

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores [CERT.br a]. Em geral, toda situação onde uma entidade de informação está sob risco é considerado um incidente de segurança. Exemplos comuns de incidentes incluem:

1. O desfiguramento do portal *web* de uma instituição;
2. A evasão de informações confidenciais;
3. A propagação de um vírus ou *worm* por meio da lista de contatos de e-mails;
4. Envio de *spam*.

Essas situações são incidentes sérios e podem facilmente resultar num impacto significativo para uma instituição, se não manejados de forma correta. De fato, a severidade de um incidente é mensurada segundo o impacto que o mesmo causa no processo de negócio de uma instituição. Por exemplo, um incidente que indisponibiliza o acesso ao *site* de uma loja virtual possui alta severidade, já que os clientes não podem acessar o *site* para realizar compras. Os incidentes de segurança podem ser classificados basicamente em duas categorias: incidentes internos e incidentes externos.

Os incidentes externos caracterizam-se por serem originados fora da rede da instituição, ou seja, externos ao domínio administrativo da instituição. Por exemplo, uma varredura por vulnerabilidades a um servidor da corporação. Ao passo que os incidentes internos referem-se a todo tipo de incidente originado na própria rede da instituição, como por exemplo, roubo de informações confidenciais e a má utilização dos recursos disponíveis.

Os incidentes de segurança internos podem ser mais dispendiosos que os incidentes externos. Esse tipo de incidente possui uma maior probabilidade de sucesso, pois se pressupõe que o atacante possui prévio conhecimento da estrutura interna da instituição. Os ataques internos, sobretudo em instituições federais - onde existem muitos alunos realizando experimentos e testando ferramentas sem a devida precaução de segurança - são muitos comuns. O potencial de um ataque interno é muito alto, uma vez que essas máquinas estão dispostas em canais de alta velocidade e com razoável poder de processamento. Esse tipo de ataque merece uma atenção especial na estrutura de segurança da universidade, sendo prudente desenvolver mecanismos especiais para sua mitigação.

Todo incidente deve ser tratado seguindo uma metodologia previamente definida pela instituição. Essa metodologia é chamada de processo de resposta a incidentes de segurança.

3. Resposta a incidentes de segurança

Resposta a incidentes de segurança é uma metodologia organizada para gerir conseqüências de uma violação de segurança da informação [CERT/CC]. O principal objetivo do processo de resposta a incidentes de segurança é minimizar o impacto de um incidente e permitir o restabelecimento dos sistemas o mais rápido possível.

Um bom plano de resposta a incidente passa pela definição de uma política de segurança, que define claramente as etapas do processo que devem ser seguidos quando um incidente ocorrer. O processo de resposta a incidentes deve ser produto de uma sinergia entre as diferentes equipes organizacionais, agregando níveis gerenciais a níveis técnicos, ao passo que a sua implementação é de responsabilidade do time de resposta a incidentes, ou CSIRT (*Computer Security Incidente Response Team*). Um time de resposta a incidentes de segurança é constituído por um grupo cuidadosamente selecionado que, além de analistas de segurança, pode incluir representantes legais e integrantes do departamento de relações públicas.

A definição de um processo de resposta a incidentes deve observar alguns princípios que norteiam a concepção de um sistema de tratamento a incidentes. Segundo os autores Kenneth Wyk e Richard Forno [Kenneth R. Wyk 2001], o processo de resposta a incidentes de segurança deve possuir cinco etapas:

1. **Identificação**: cabe a esta etapa detectar ou identificar de fato a existência de um incidente de segurança. Para isso a equipe pode basear-se em notificações externas ou num conjunto de ferramentas de monitoração de rede, como um IDS (sistema de detecção de intrusão). Os esforços da equipe concentram-se em identificar os sintomas do ataque e suas características, observando a severidade do incidente, ou seja, o quanto a estrutura de negócios da instituição é afetada. Recomenda-se também que o time de resposta a incidentes implemente uma base de conhecimento de incidentes, isto é, um conjunto de registros de incidentes passados. Essa base de conhecimento será útil para levantar informações iniciais dos incidentes em andamento, assim como sintomas e características.
2. **Coordenação**: após identificar a existência de um incidente e suas conseqüências na etapa anterior, cabe à equipe identificar os danos causados pelo incidente em questão. A avaliação dos sintomas coletados permite diagnosticar de forma preliminar a causa do problema, ou pelo menos inferir algumas conclusões que serão úteis para determinar a ação a ser tomada. De forma conclusiva, esta etapa sugere possíveis ações que possivelmente podem resolver o incidente em andamento.
3. **Mitigação**: o objetivo desta etapa é isolar o problema e determinar a extensão dos danos através da implementação da solução delineada na etapa anterior. Além de utilizar procedimentos para isolar o incidente - evitando a propagação do ataque -, a equipe também busca restabelecer o sistema, mesmo que seja com uma solução temporária, até que a solução definitiva seja implementada.
4. **Investigação**: nesta etapa, o time de resposta concentra-se em coletar e analisar as evidências do incidente de segurança. O processamento de evidências como registros, arquivos de pacotes capturados e até mesmo entrevistas com os responsáveis são muito importantes para a resolução de futuros incidentes com características semelhantes.
5. **Educação**: esta etapa consiste em avaliar o processo de tratamento de incidentes e verificar a eficácia das soluções implementadas. As lições aprendidas durante todo o processo devem ser propagadas para toda a equipe, descrevendo formas de obter melhores resultados e até mesmo recomendações aos usuários.

4. A operação de resposta a incidentes de segurança

A operação do processo de resposta a incidentes de segurança tem o objetivo de pôr em prática toda a metodologia descrita no plano de resposta a incidentes. Um consistente plano de resposta afeta diretamente a qualidade do procedimento operacional realizado pela equipe de segurança. Diante disso, essa seção irá descrever em linhas gerais como o processo de resposta a incidentes de segurança foi operacionalizado na Universidade Federal do Rio Grande do Sul e também irá apresentar resultados da implementação.

Toda atividade de resposta é liderada pelo time de resposta a incidentes de segurança, denominado TRI (**Time de Resposta a Incidentes**), o qual é composto por 3 pessoas. O time concentra-se unicamente no processo de resposta a incidentes, ou seja, é responsável por tratar todo incidente notificado ou detectado pela própria equipe de segurança.

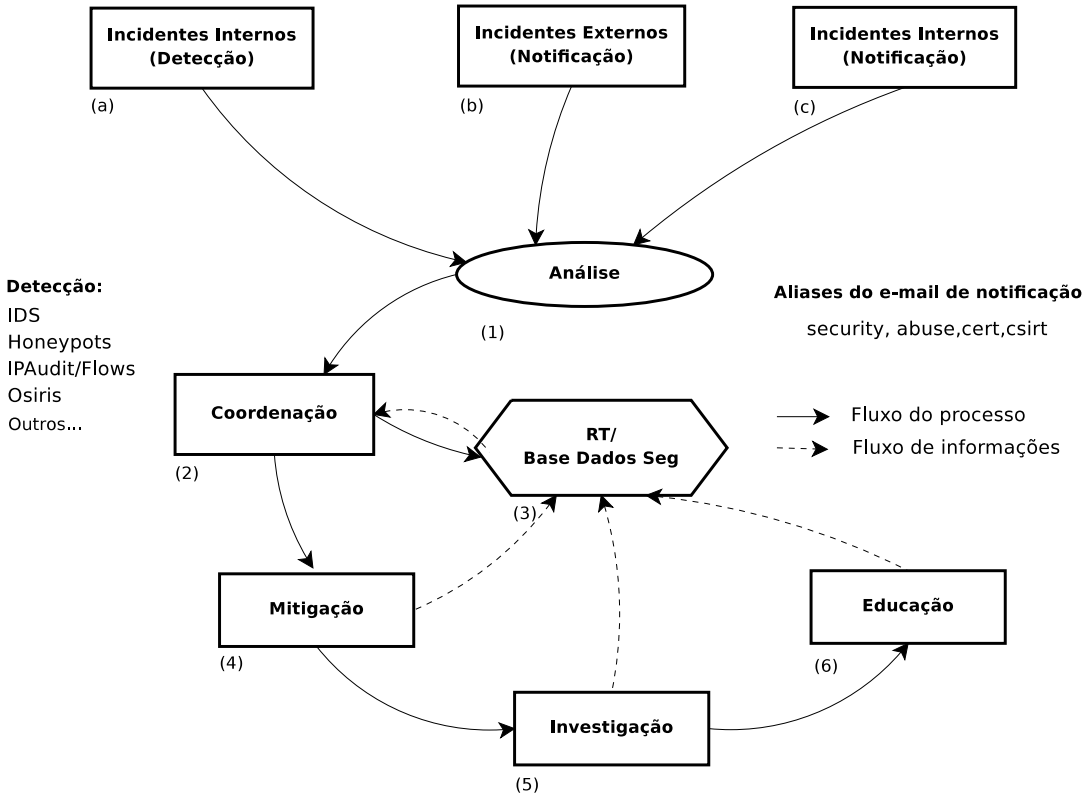

Figura 1. Processo de tratamento de incidentes de segurança

A figura 1 busca ilustrar as várias etapas que um incidente passa até ser completamente resolvido na Universidade Federal do Rio Grande do Sul. Como pode ser visto na parte superior da figura, são apresentados 3 blocos que correspondem ao ponto inicial de todo o processo: a suspeita de um incidente de segurança.

O bloco (a) corresponde à detecção de um incidente observado pela própria equipe. Isso acontece através da correlação de dados de diferentes ferramentas de segurança. Ferramentas como IDS (*Intrusion Detection System*) e HIDS (*Host intrusion detecion system*), observação dos acessos aos honeypots e mapeamento de conexões via fluxos de rede, são recursos de segurança utilizados pela equipe da UFRGS e compõem uma

solução que vem se demonstrando eficaz. Os processos (b e c) da figura correspondem a notificações oriundas de usuários locais ou entidades externas da rede. Essas notificações geralmente são recebidas via e-mail, direcionadas à caixa postal do grupo de segurança. As notificações também podem ser feitas via telefone, fax ou até mesmo contato pessoal. Até o presente momento, os incidentes reportados via notificação são apenas suspeitas e só serão confirmados após uma análise (1). Na etapa (1), se a equipe constata a existência de um incidente, o incidente é encaminhado para a etapa (2).

Na etapa 2, a equipe é responsável por identificar o problema, definindo a causa ou o motivo pelo qual o incidente foi gerado. Esta etapa é realizada observando as características do ataque em andamento e também consultando uma base de dados de segurança (3), a qual disponibiliza incidentes prévios que podem ser úteis para a resolução do problema. Por exemplo, no caso de uma máquina comprometida, a equipe irá levantar informações dos *logs* do sistema comprometido e também do sistema de IDS. Em adição, uma consulta à base de dados de segurança pode ser útil para encontrar possíveis soluções que foram utilizadas em incidentes semelhantes. A rigor, a equipe busca esboçar possíveis soluções que resolvam o incidente atual.

Na etapa 4, são implementadas medidas visando isolar as causas e minimizar as conseqüências do incidente. Para isso, a equipe vale-se de ferramentas da infra-estrutura da rede, como *firewalls*, roteadores e IDS. Por exemplo, num incidente onde exista uma varredura por vulnerabilidades a equipe de segurança pode, num primeiro momento, aplicar filtros no *firewall* ou até mesmo isolar uma sub-rede através de filtros no roteador. Após o incidente ter sido mitigado, a equipe concentra-se na investigação (5) do problema, buscando documentar todo processo na base de dados de segurança (3). Informações como características, métodos utilizados para mitigação, serviços atacados e responsáveis pelo sistema são inseridos na base de dados, para que possam ser úteis na resolução de outros incidentes, além de fomentar as estatísticas de incidentes da própria instituição.

A etapa (6), educação, é destinada a propagar as informações aprendidas durante todo o processo de tratamento de um incidente de segurança. Geralmente é realiza através da emissão de alertas para comunidade acadêmica e também no desenvolvimento de documentos visando boas práticas de segurança.

As etapas descritas acima apresentam em linhas gerais como o processo de resposta a incidentes de segurança é realizado pela equipe pelo TRI, time de resposta da UFRGS. Na seqüência, são apresentados alguns números de incidentes, buscando apresentar o volume de informação tratado pela equipe.

4.1. Resultados

A reformulação do processo de tratamento de incidentes de segurança da UFRGS ocorreu em novembro de 2008, logo os resultados apresentados nesta seção correspondem aos meses de dezembro de 2008 e janeiro e fevereiro de 2009. Embora esse período seja uma época de férias - com exceção de dezembro que teve 20 dias de período letivo - é possível ter uma noção do volume e características dos incidentes tratados. Na figura 2, são apresentados os incidentes, agrupados por mês e por características de origem. Os incidentes do tipo *detectados/internos* correspondem a ataques detectados pela equipe ou diretamente reportados por clientes da rede; já os externos, são os incidentes notificados por entidades externas à rede local, como outros times de respostas. No mês de dezembro

constatou-se o maior volume de incidentes, totalizando 330 incidentes, sendo 297 internos e apenas 33 incidentes externos. Em janeiro, foram tratados um total de 233 incidentes, com 184 internos e 49 externos. Por último, em fevereiro, foram tratados 195 incidentes, sendo 166 internos e 29 externos.

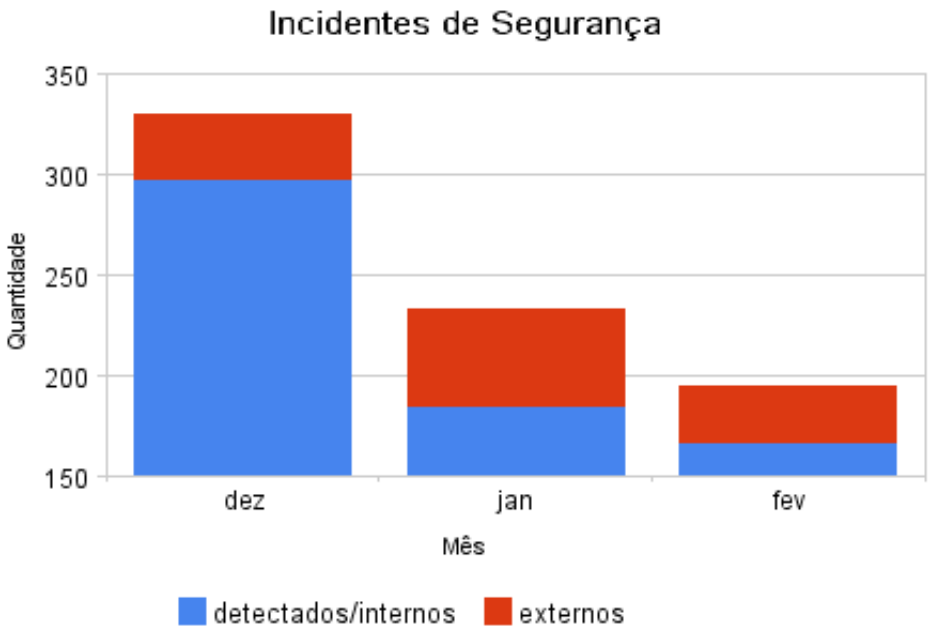

Figura 2. Número de incidentes e origem da notificação

Os resultados acima demonstram o grande volume de incidentes tratados pelo time de resposta. Embora os resultados tenham sido coletados num período de pouca atividade estudantil, é possível demonstrar que grande parte dos incidentes tratados são de origem interna, ou seja, são detectados pela equipe ou notificados pelos próprios usuários. As estatísticas do tratamento de incidentes internos sugerem que as primeiras etapas do processo estão sendo funcionais, não permitindo que os ataques se alastrem para fora da rede o que, em caso contrário, resultaria num grande volume de notificações externas.

5. Conclusão e Considerações Finais

Este trabalho discute o processo de resposta a incidentes de segurança, especificamente em instituições de ensino. Para isto, este trabalho debate as necessidades pontuais das instituições de ensino no que tange a segurança da informação, levando em conta a sua complexidade para a implementação de um plano de resposta a incidentes. Os autores apresentam a implementação do processo de tratamento a incidentes de segurança tendo em vista os modelos propostos por órgãos reguladores, como o CERT-CC. Cada etapa do processo é descrita e são apontadas soluções que o time de segurança da UFRGS utiliza corriqueiramente para solucionar os eventuais problemas. Por fim, o trabalho apresenta como o fluxo de informações ocorre durante todo o processo e apresenta números que confirmam que o processo implementado consegue atender as necessidades da instituição.

Como trabalho futuro a equipe deseja aprimorar o processo, automatizando algu-

mas tarefas e gerando estatísticas de forma automatizada, possibilitando o acompanhamento dos incidentes de segurança e até mesmo possíveis tendências dos incidentes.

Referências

CERT.br. Cartilha de Segurança para Internet. Disponível em: http://www.cert.br/cartilha. Acesso em: Março de 2009.

CERT.br. Estatísticas dos Incidentes Reportados ao CERT.br. Disponível em: http://www.cert.br/stats. Acesso em: Março de 2009.

CERT/CC. Computer Security Incident Response Team FAQ. Disponível em: http://www.cert.org/csirts/csirt-faq.html. Acesso em: Março de 2008.

FIRST. FIRST Best Practice Guide Library. Disponível em: http://www.first.org. Acesso em: Março de 2008.

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