Cartilha de Segurança para Internet

Parte VII: Incidentes de Segurança e Uso Abusivo da Rede

Versão 3.0
Setembro de 2005
http://cartilha.cert.br/

CERT.br – Centro de Estudos, Resposta e Tratamento
de Incidentes de Segurança no Brasil

Cartilha de Segurança para Internet

Parte VII: Incidentes de Segurança e Uso Abusivo da Rede

Esta parte da Cartilha aborda tópicos relativos a incidentes de segurança e uso abusivo da rede. São discutidos os conceitos de política de segurança, política de uso aceitável, registros de eventos e sistemas de detecção de intrusão. Também são discutidos os procedimentos relativos ao processo de identificação e notificação de incidentes de segurança.

Versão 3.0 – Setembro de 2005
http://cartilha.cert.br/

Sumário

1 Incidentes de Segurança e Abusos

1.1 O que é incidente 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.

São exemplos de incidentes de segurança:

- tentativas de ganhar acesso não autorizado a sistemas ou dados;
- ataques de negação de serviço;
- uso ou acesso não autorizado a um sistema;
- modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema;
- desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

1.2 O que é política de segurança?

A política de segurança atribui direitos e responsabilidades às pessoas que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também define as atribuições de cada um em relação à segurança dos recursos com os quais trabalham.

Uma política de segurança também deve prever o que pode ser feito na rede da instituição e o que será considerado inaceitável. Tudo o que descumprir a política de segurança pode ser considerado um incidente de segurança.

Na política de segurança também são definidas as penalidades às quais estão sujeitos aqueles que não cumprirem a política.

1.3 O que é política de uso aceitável (AUP)?

A política de uso aceitável (AUP, de *Acceptable Use Policy*) é um documento que define como os recursos computacionais de uma organização podem ser utilizados. Também é ela quem define os direitos e responsabilidades dos usuários.

Os provedores de acesso a Internet normalmente deixam suas políticas de uso aceitável disponíveis em suas páginas. Empresas costumam dar conhecimento da política de uso aceitável no momento da contratação ou quando o funcionário começa a utilizar os recursos computacionais da empresa.

1.4 O que pode ser considerado uso abusivo da rede?

Não há uma definição exata do que possa ser considerado um uso abusivo da rede.

Internamente às empresas e instituições, situações que caracterizam o uso abusivo da rede estão definidas na política de uso aceitável. Na Internet como um todo, os comportamentos listados abaixo são geralmente considerados como uso abusivo:

- envio de *spam* (mais informações na parte VI: *Spam*);
- envio de correntes da felicidade e de correntes para ganhar dinheiro rápido (mais informações na parte IV: Fraudes na Internet);
- envio de *e-mails* de *phishing/scam* (mais informações na parte IV: Fraudes na Internet);
- cópia e distribuição não autorizada de material protegido por direitos autorais;
- utilização da Internet para fazer difamação, calúnia e ameaças;
- ataques a outros computadores;
- comprometimento de computadores ou redes.

2 Registros de Eventos (*logs*)

2.1 O que são *logs*?

Os *logs* são registros de atividades gerados por programas de computador. No caso de *logs* relativos a incidentes de segurança, eles normalmente são gerados por *firewalls*[1] ou por sistemas de detecção de intrusão.

2.2 O que é um sistema de detecção de intrusão (IDS)?

Um sistema de detecção de intrusão (IDS – *Intrusion Detection System*) é um programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas.

IDSs podem ser instalados de modo a monitorar as atividades relativas a um computador ou a uma rede.

2.3 Que tipo de atividade pode ocasionar a geração de um *log*?

Os *firewalls*, dependendo de como foram configurados, podem gerar *logs* quando alguém tenta acessar um computador e este acesso é barrado pelo *firewall*. Sempre que um *firewall* gera um *log* informando que um determinado acesso foi barrado, isto pode ser considerado uma tentativa de invasão, mas também pode ser um falso positivo (vide seção 2.4).

Já os sistemas de detecção de intrusão podem gerar *logs* tanto para casos de tentativa de invasão, quanto para casos em que um ataque teve sucesso. Apenas uma análise detalhada pode dizer se uma atividade detectada por um IDS foi um ataque com sucesso. Assim como os *firewalls*, os sistemas de detecção de intrusão também podem gerar falsos positivos.

[1] Maiores detalhes na seção *Firewalls* da parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção.

2.4 O que é um falso positivo?

O termo "falso positivo" é utilizado para designar uma situação em que um *firewall* ou IDS aponta uma atividade como sendo um ataque, quando na verdade esta atividade não é um ataque.

Um exemplo clássico de falso positivo ocorre no caso de usuários que costumam se conectar em servidores de IRC e que possuem um *firewall* pessoal. Atualmente boa parte dos servidores de IRC possui uma política de uso que define que um usuário, para se conectar em determinados servidores, não deve possuir em sua máquina pessoal nenhum *software* que atue como *proxy*[2]. Para verificar se um usuário tem algum *software* deste tipo, ao receberem uma solicitação de conexão por parte de um cliente, os servidores enviam para a máquina do cliente algumas conexões que checam pela existência destes programas. Se o usuário possuir um *firewall* é quase certo que estas conexões serão apontadas como um ataque.

Outro caso comum de falso positivo ocorre quando o *firewall* não está devidamente configurado e indica como ataques respostas a solicitações feitas pelo próprio usuário.

2.5 Que tipo de informação está presente em um *log*?

Os *logs* relativos a ataques recebidos pela rede, em geral, possuem as seguintes informações:

- Data e horário em que ocorreu uma determinada atividade;
- Endereço IP[3] de origem da atividade;
- Portas envolvidas;

Dependendo do grau de refinamento da ferramenta que gerou o *log* ele também pode conter informações como:

- O *time zone*[4] do horário do *log*;
- Protocolo utilizado (TCP, UDP, ICMP, etc).
- Os dados completos que foram enviados para o computador ou rede.

3 Notificações de Incidentes e Abusos

3.1 Por que devo notificar incidentes?

Quando um ataque é lançado contra uma máquina ele normalmente tem uma destas duas origens:

[2] A definição de *proxy* pode ser encontrada no Glossário.
[3] A definição de endereço IP pode ser encontrada no Glossário.
[4] Fuso horário. Mais informações em http://www.cert.br/docs/faq1.html.

- um programa malicioso que está fazendo um ataque de modo automático, como por exemplo um *bot* ou um *worm*[5];
- uma pessoa que pode estar ou não utilizando ferramentas que automatizam ataques.

Quando o ataque parte de uma máquina que foi vítima de um *bot* ou *worm*, reportar este incidente para os responsáveis pela máquina que originou o ataque vai ajudá-los a identificar o problema e resolvê-lo.

Se este não for o caso, a pessoa que atacou o seu computador pode ter violado a política de uso aceitável da rede que utiliza ou, pior ainda, pode ter invadido uma máquina e a utilizado para atacar outros computadores. Neste caso, avisar os responsáveis pela máquina de onde partiu o ataque pode alertá-los para o mau comportamento de um usuário ou para uma invasão que ainda não havia sido detectada.

3.2 Para quem devo notificar os incidentes?

Os incidentes ocorridos devem ser notificados para os responsáveis pela máquina que originou a atividade e também para os grupos de resposta a incidentes e abusos das redes envolvidas. De modo geral a lista de pessoas/entidades a serem notificadas inclui:

- os responsáveis pela rede que originou o incidente, incluindo o grupo de segurança e abusos, se existir um para aquela rede;
- o grupo de segurança e abusos da rede em que você está conectado (seja um provedor, empresa, universidade ou outro tipo de instituição);

Mantenha o CERT.br (cert@cert.br) na cópia da mensagem, caso algum dos *sites* envolvidos seja brasileiro.

3.3 Por que devo manter o CERT.br na cópia das notificações?

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br[6]), mantido pelo Comitê Gestor da Internet no Brasil (CGI.br), é responsável pelo tratamento de incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil.

Dentre as atribuições do CERT.br estão:

- ser um ponto central para notificações de incidentes de segurança no Brasil, de modo a prover a coordenação e o apoio no processo de resposta a incidentes, colocando as partes envolvidas em contato quando necessário;
- manter estatísticas sobre os incidentes a ele reportados[7];

[5] Mais detalhes sobre *bot* e *worm* estão na parte VIII: Códigos Maliciosos (*Malware*).
[6] Anteriormente denominado NBSO – NIC BR *Security Office*.
[7] http://www.cert.br/stats/

- desenvolver documentação[8] de apoio para usuários e administradores de redes Internet.

Manter o CERT.br nas cópias das notificações de incidentes de segurança é importante para permitir que:

- as estatísticas geradas reflitam os incidentes ocorridos na Internet brasileira;
- o CERT.br escreva documentos direcionados para as necessidades dos usuários da Internet no Brasil;
- o CERT.br possa correlacionar dados relativos a vários incidentes, identificar ataques coordenados, novos tipos de ataques, etc.

3.4 Como encontro os responsáveis pela máquina de onde partiu um ataque?

Na Internet são mantidas diversas bases de dados com as informações a respeito dos responsáveis por cada bloco de números IP[9] existente. Estas bases de dados estão nos chamados "Servidores de *Whois*".

O servidor de *Whois* para os IPs alocados ao Brasil pode ser consultado em `http://registro.br/`. Para os demais países e continentes existem diversos outros servidores. O *site* `http://www.geektools.com/whois.php` aceita consultas referentes a qualquer número IP e redireciona estas consultas para os servidores de *Whois* apropriados.

Os passos para encontrar os dados dos responsáveis incluem:

- Acessar o *site* `http://registro.br/` e fazer uma pesquisa pelo número IP ou pelo nome de domínio da máquina de onde partiu a atividade;
- Se o IP da máquina estiver alocado para o Brasil, os dados dos responsáveis serão exibidos;
- Se aparecer a mensagem: "`Não alocado para o Brasil`", significa que o IP está alocado para algum outro país. Uma consulta no *site* `http://www.geektools.com/whois.php` pode retornar os *e-mails* dos responsáveis.

Vale lembrar que os *e-mails* que são encontrados a partir destas consultas não são necessariamente os *e-mails* da pessoa que praticou o ataque. Estes *e-mails* são dos responsáveis pela rede onde a máquina está conectada, ou seja, podem ser os administradores da rede, sócios da empresa, ou qualquer outra pessoa que foi designada para cuidar da conexão da instituição com a Internet.

3.5 Que informações devo incluir em uma notificação de incidente?

Para que os responsáveis pela rede de onde partiu o incidente possam identificar a origem da atividade é necessário que a notificação contenha dados que permitam esta identificação.

São dados essenciais a serem incluídos em uma notificação:

[8] `http://www.cert.br/docs/`
[9] O conceito de número IP pode ser encontrado no Glossário.

- *logs* completos;
- data, horário e *time zone* (fuso horário) dos *logs* ou da ocorrência da atividade sendo notificada;
- dados completos do incidente ou qualquer outra informação que tenha sido utilizada para identificar a atividade.

3.6 Como devo proceder para notificar casos de *phishing/scam*?

Um caso de *phishing/scam* deve ser tratado de forma diferente de outros tipos de incidente, pois não necessariamente haverá *logs* gerados por um *firewall* ou IDS, por exemplo.

O *phishing/scam* é uma mensagem de *e-mail* que procura induzir o usuário a fornecer dados pessoais e financeiros. Desta forma, uma notificação de incidente deste tipo deve conter o cabeçalho e conteúdo completos da mensagem recebida pelo usuário.

A notificação deve ser enviada para os responsáveis pelas redes envolvidas, mantendo o CERT.br (cert@cert.br) na cópia da mensagem de notificação. As informações de contato dos responsáveis pelas redes envolvidas, ou seja, do servidor de onde partiu o *e-mail* e do *site* que está hospedando o esquema fraudulento, devem ser obtidas no cabeçalho e conteúdo da mensagem de *phishing/scam*.

Mais detalhes sobre *phishing/scam* podem ser obtidos na parte IV: Fraudes na Internet. Informações sobre somo obter cabeçalhos e conteúdos completos de mensagens de *e-mail* podem ser encontradas na parte VI: *Spam*.

3.7 Onde posso encontrar outras informações a respeito de notificações de incidentes?

O CERT.br mantém uma FAQ (*Frequently Asked Questions*) com respostas para as dúvidas mais comuns relativas ao processo de notificação de incidentes. A FAQ pode ser encontrada em: http://www.cert.br/docs/faq1.html.

Como Obter este Documento

Este documento pode ser obtido em http://cartilha.cert.br/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@cert.br.

Nota de *Copyright* e Distribuição

Agradecimentos

O CERT.br agradece a todos que contribuíram para a elaboração deste documento, enviando comentários, críticas, sugestões ou revisões.