GRIS-UFRJ

Bruno Salgado Guimarães
Aluno do curso de Ciência da Computação da UFRJ e Diretor do GRIS-UFRJ.

O Grupo de Respostas a Incidentes de Segurança do DCC-UFRJ (GRIS-UFRJ) e a Importância dos CSIRTs

O GRIS, Grupo de Resposta a Incidentes de Segurança, criado pelos alunos da graduação do curso de Ciência da Computação da UFRJ em novembro de 2003 e formalizado pelo Departamento de Ciência da Computação da UFRJ em maio de 2004, tem como objetivo a detecção, resolução e prevenção de incidentes de segurança na UFRJ, além de oferecer suporte acadêmico aos estudantes de computação e demais alunos interessados nos assuntos relacionados à segurança da informação.

O GRIS atua nos moldes de um CSIRT (Computer Security Incident Response Team), um grupo em atividade que visa receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança e divulgar práticas e recomendações de redes e sistemas. O grupo hoje conta com uma equipe de 20 pessoas, sendo 15 membros ativos e 5 colaboradores, coordenado pelo Prof. Nelson Quilula Vasconcellos do DCC-UFRJ e orientado por Carlos Mendes, analista de segurança do NCE.

O GRIS tem atuado constantemente no Departamento de Ciência da Computação da UFRJ e no Instituto de Geociências da UFRJ, e eventualmente em outros departamentos e unidades quando solicitado. Em abril, foi aberto o primeiro processo seletivo, que mesmo não oferecendo bolsas-auxílio para os estudantes, contou com 34 alunos de 4 cursos de graduação da UFRJ, resultando na seleção de 9 novos membros.

Um dos principais objetivos do GRIS é sanar a carência de estudo e pesquisa na área de segurança da informação não só na UFRJ, mas nas demais universidades do Estado do Rio de Janeiro. Com a criação de CSIRTs universitários, os alunos são estimulados a realizarem pesquisa e desenvolvimento na área, que são remetidos a comunidade sob a forma de artigos, alertas, recomendações, ferramentas, tutoriais, entre outros serviços. Além disso, os alunos têm a oportunidade de estar em contato direto com pessoas que dividem interesses comuns na área de segurança, possibilitando aprendizado rápido e direcionado, e de participar ativamente de um CSIRT, seja como membros ou colaboradores.

DEFINIÇÃO DE UM CSIRT

Um CSIRT é um grupo ou organização que provê serviços e suporte para um público bem definido, para tratamento, prevenção, divulgação e resposta a incidentes de segurança.
Existem dois modelos básicos de atuação para os CSIRTs. Os grupos formados em caráter definitivo e constante, atuando de forma contínua, mesmo quando não há incidentes de segurança, e os chamados grupos temporários, que se reúnem somente quando há uma incidente de segurança em andamento ou para responder a um incidente específico.

DEFINIÇÃO DE INCIDENTE DE SEGURANÇA

De uma forma generalizada, incidentes de segurança podem ser definidos como uma atividade nas máquinas ou na rede que possa ameaçar a segurança dos sistemas computacionais. Na prática, cada organização deve definir as suas prioridades e sua própria definição e formatação de incidente.

Entre inúmeras possibilidades de definições de incidentes, podemos citar algumas, tais como:

- modificações nas características de hardware e software de um sistema, sem o conhecimento ou consentimento prévio do responsável ou responsáveis pelo sistema
- tentativas (com ou sem sucesso) de ganhar acesso não autorizado a sistemas ou a seus dados
- utilização dos recursos da rede para atividades não autorizadas
- interrupção indesejada da rede, seja causada por meio físico, lógico ou ambos
- negação de serviço (tirar de operação um ou mais serviços ou computadores conectados à Internet, através de ataques provenientes de um ou mais computadores)

Um dos princípios básicos para a criação e funcionamento de um CSIRT é a exata definição das atividades que podem ser consideradas incidentes de segurança, o que vai variar de acordo com cada organização. Máquinas clientes alocadas nas extremidades das mesas, acessos a sites externos não autorizados, cabos sem a devida proteção soltos em ambientes de circulação de pessoal, uso excessivo da rede ou uso excessivo do sistema para armazenamento de dados até uma tentativa de ganhar acesso não autorizado a um sistema podem ser considerados incidentes de segurança. Cabe a cada CSIRT, de acordo com seus objetivos, elaborar seu próprio estatuto.

IMPORTÂNCIA DE UM CSIRT PARA AS ORGANIZAÇÕES E ALGUMAS DE SUAS PRINCIPAIS CARACTERÍSTICAS

Mesmo a melhor infra-estrutura de segurança da informação não pode garantir que intrusões ou outras ações maliciosas ocorrerão. Por outro lado, essa mesma estrutura talvez não consiga evitar que incidentes sem intenções "maléficas" possam vir a acontecer, seja por descuido, falta de conhecimento ou treinamento inadequado dos usuários, podendo igualmente acarretar graves danos e conseqüências para a organização.

A agilidade com que a organização pode detectar, analisar e responder a um incidente de segurança limita os danos e diminui o custo e o tempo do processo de recuperação. Um CSIRT pode estar fisicamente presente e apto a conduzir uma resposta imediata para conter o incidente de segurança e para iniciar o processo de recuperação. CSIRTs também estarão familiarizados com os sistemas comprometidos, e, portanto, melhor preparados para coordenar e propor estratégias de erradicação e resposta aos problemas.

CSIRTs podem e devem atuar também de forma pró-ativa, elaborando políticas de segurança, planos de continuidade, divulgação de alertas e vulnerabilidades com suas devidas recomendações, treinamento e desenvolvimento de ferramentas e sistemas personalizados para a organização em que atuam, diminuindo assim a probabilidade do acontecimento de incidentes de segurança.

A centralização da comunicação e registro dos incidentes e soluções de segurança em uma única localidade (seja físico ou lógico) é altamente benéfico para a organização. Quando todos os incidentes são reportados ao CSIRT (ou conglomerado de CSIRTs) da organização, as soluções são elaboradas e automaticamente encaminhadas a qualquer parte da organização que possua a mesma atividade/ocorrência de incidentes (seja como forma de execução da solução, ou prestação de consultoria ou suporte, dependendo do formato do CSIRT perante a organização). Com essa centralização de informações, o CSIRT pode elaborar planos e estratégias para os incidentes mais comuns e/ou mais graves com ainda mais agilidade, através do estudo da estatística dos incidentes reportados, e o impacto causado. Uma organização pode possuir mais de um CSIRT em atuação, embora seja recomendado que a coordenação geral seja realizada por uma equipe bem definida.

Um CSIRT deve também ter um relacionamento amplo e direto com outros CSIRTS, sejam internos ou externos, e com organizações de segurança, visando facilitar o compartilhamento de estratégias de respostas e geração de alertas para potenciais problemas. Pode também trabalhar em conjunto com outras áreas da organização de maneira pró-ativa, garantindo que novos sistemas sejam desenvolvidos e colocados em produção, tendo a preocupação com a segurança e em conformidade com as políticas de segurança vigentes, facilitando inclusive a detecção das áreas vulneráveis da organização e a realização da análise de vulnerabilidades e detecção de incidentes.

REFERÊNCIAS

Maiores detalhes sobre O GRIS-UFRJ podem ser encontradas em : www.gris.dcc.ufrj.br

Mais informações sobre CSIRTs nacionais e internacionais e assuntos relacionados podem ser encontrados nos links listados em: www.gris.dcc.ufrj.br/grupos.php