Recomendação de Segurança 002/2012 - CGTI/VPGDI

Em 16 de janeiro de 2012

Para: Gestores de TI das unidades da Fiocruz
Assunto: Registro de Logs

Prezado Gestor,

O gerenciamento de log é extremamente importante para administração segura de rede e sistemas, por registrar informações sobre o seu funcionamento e principalmente para o monitoramento da segurança, possibilitando assim a coleta e retenção de evidência para registro e tratamento de incidentes.

O log pode ser utilizado para investigação como evidência em casos legais ou disciplinares. Registros (log) incorretos podem impedir tais investigações e causar danos à credibilidade das evidências.

Sendo assim, com base na ABNT NBR ISO/IEC 27002, o Serviço de Segurança da Informação e Comunicações recomenda que:

a) Os registros (log) sejam protegidos contra falsificação, acesso indevido e modificações, tais como:
    i. Alterações dos tipos de mensagens que são gravadas;
    ii. Arquivos de registros (log) sendo editados ou excluídos;
    iii. Capacidade de armazenamento da mídia magnética do arquivo de registros (log) excedida, resultando em falhas no registro de eventos ou sobreposição do registro de evento anterior.
b) Os registros (log) contenham as seguintes informações:
    i. A hora em que o evento ocorreu (sucesso ou falha);
    ii. Informações sobre o evento (exemplo: arquivos manuseados) ou falha (exemplo: erros ocorridos e ações corretivas adotadas);
    iii. Conta e administrador/operador envolvido;
    iv. Quais processos estavam envolvidos.

c) Os horários de servidores sejam sincronizados via NTP, para garantir a exatidão dos registros (log);
d) Os registros (log) sejam analisados com frequência;
e) Os registros (log) façam parte da rotina de cópia de segurança, com nível apropriado de proteção física/ambiental e testado periodicamente;
f) Os registros (log) sejam armazenados em *loghost* [1] centralizado (todos os logs em um mesmo servidor), dedicado (não disponibiliza nenhum outro serviço) e sem acesso remoto, a fim de minimizar a possibilidade de comprometimento das informações.
g) Os registros (log) sejam preservados por um período mínimo de seis meses;
h) Os registros (log) sejam incluídos no procedimento de backup.

Atenciosamente,

Misael Sousa de Araujo
Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações

[1] *Loghost* é um sistema dedicado à coleta e ao armazenamento de logs de outros sistemas em uma rede, servindo como um repositório redundante de logs.