

Como prevenir os crimes da era digital

Devido à era digital, as empresas estão cada vez mais dependentes de sistemas para realizarem suas tarefas, mensurar os lucros e as despesas de maneira clara, rápida e objetiva.

Porém devemos nos preocupar com a segurança dessas informações, pois são dados importantes para o negócio, e caindo em mãos erradas podem acarretar prejuízos ou até quebra da empresa. Por isso a necessidade da existência de departamentos de auditoria interna focado nos sistemas e infra-estrutura que armazenam e transporta essas informações. Na figura 1, demonstramos o escopo da auditoria de sistema que são baseados e controles de TI.

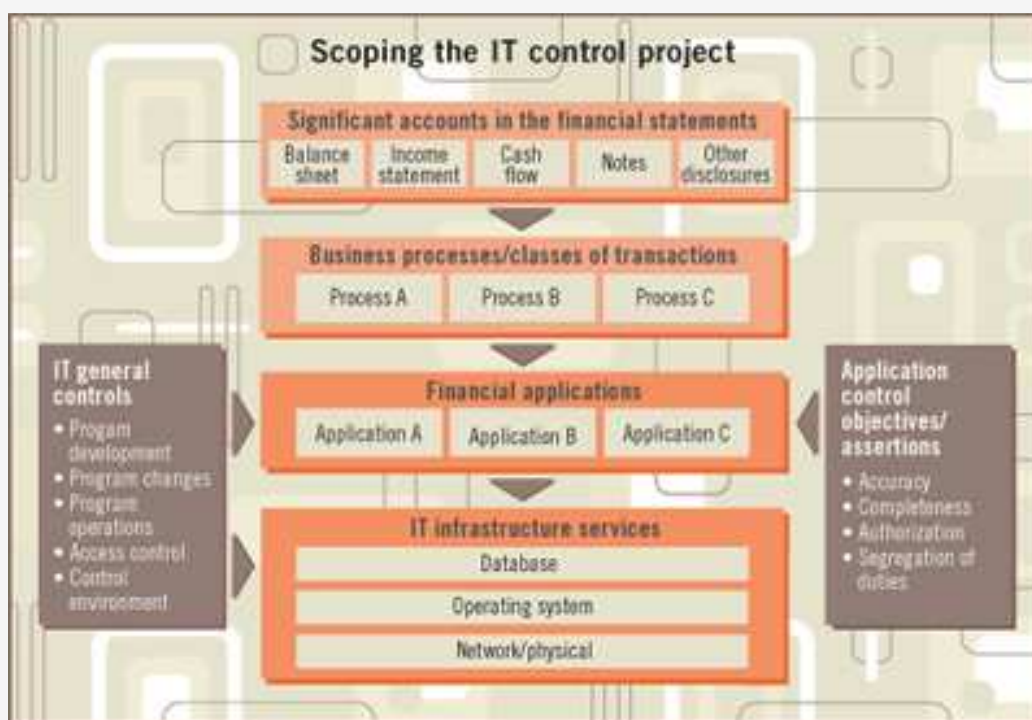


Figura 1

Nas auditorias de sistemas convencionais são verificados: Controle de acesso físico e lógico, gerenciamento de mudanças de sistema, gerenciamento de antivírus, backup e restore e gerenciamento do ambiente de TI, mas com adversidade de tecnologias acessando emails, sistemas internos e as redes empresariais, devemos nos preocupar um pouco mais. Abaixo temos um caso de problema de segurança de sistemas:

Site do IBGE é alvo de defacing

(<http://idgnow.uol.com.br/internet/2011/06/24/site-do-ibge-e-alvo-de-defacing>)

Por Redação IDGNow!

Publicada em 24 de junho de 2011 às 08h27

Atualizada em 24 de junho de 2011 às 08h46

Ao pé da página, hackers negam ter relações com os grupos LulzSec ou Anonymous no Brasil.

O site do Instituto Brasileiro de Geografia e Estatística (IBGE) (www.ibge.gov.br) teve sua página inicial modificada no início sexta-feira (24/6). A imagem da bandeira do Brasil, assinada por um grupo que se intitula "FIREH4CK3R", contém mensagens de cunho nacionalista, típicas de outros ataques do grupo. Recentemente, eles já haviam invadido o site da embaixada norte-americana no Brasil.

A invasão e o defacing foram confirmados pela assessoria do IBGE. A página modificada ficou no ar até pouco depois das 8h da manhã. Nela havia um aviso informando que neste mês o Brasil sofrerá o "maior número de ataques de natureza virtual" de sua história. E um protesto contra a ação dos grupos

LulzSecBrasil e Anonymous que ao longo dessa semana reivindicaram ataques às páginas da Presidência da República, da Receita Federal, do Ministério do Esporte e da Petrobras.

O aviso deixado pelos invasores diz que: "Este mês, o governo vivenciará o maior número de ataques de natureza virtual na sua história feito pelo fail shell. Entendam tais ataques como forma de protesto de um grupo nacionalista que deseja fazer do Brasil um país melhor. Tenha orgulho de ser brasileiro, ame o seu país, só assim poderemos crescer e evoluir. Atacado por Fireh4ck3r. Brasil, um país de todos! "Não há espaço para grupos sem qualquer ideologia como LulzSec ou Anonymous no Brasil".

O caso acima mostra problemas de segurança que muitas empresas de grande porte passam, devido à falta de uma análise a fundo das vulnerabilidades em seu ambiente tecnológico. Será que só modificaram a página? Será que tiveram acesso a informações sigilosas?

Para conseguirmos minimizar esse risco devemos incluir em nosso escopo da auditoria de sistema, o processo de realização de teste de invasão, pois assim conseguiríamos identificar as vulnerabilidades nos sistemas e na rede antes dos criminosos digitais. O que é teste de invasão, e para que serve?

Um teste de invasão, ocasionalmente, é um método de avaliar a segurança de um sistema de computador ou rede, simulando um ataque como um *Cracker*. O processo envolve uma análise ativo do sistema para identificar vulnerabilidades potenciais ou configuração inadequado do sistema, falhas de hardware ou software, ou deficiências operacionais em processo conhecidos e desconhecidos.