Os Benefícios da Política de Segurança Baseada na Avaliação de Riscos e na Integração de Ferramentas

The Benefits of the Security Politics Based on the Evaluation of Risks and the Integration of Tools

José Maurício dos Santos Pinheiro [1]

Resumo

Com a expansão das redes de comunicação, as barreiras sociais e territoriais deixaram de existir e os sistemas de informação tornaram-se acessíveis a um público cada vez maior, passando a incorporar cada vez mais novas funcionalidades. Entretanto, quanto mais recursos são requeridos para um sistema, maior será sua complexidade, maior o número de acessos disponibilizados e maiores as dificuldades para garantir sua segurança. Devido a esse fato, os ambientes computacionais passaram a ser alvo freqüente de ameaças e ataques com um grau de sofisticação crescente. Este artigo fornece uma visão geral dos impactos das invasões sobre os sistemas computacionais, abordando suas causas determinantes e predisponentes e descrevendo os elementos-chave e benefícios de uma política de segurança baseada na avaliação de riscos e na integração de ferramentas.

Palavras-chave: Segurança; Integração; Ameaças; Ataques; Vulnerabilidades.

Abstract

With the expansion of the communication nets, the social and territorial barriers vanished and the information systems became accessible to the public more and more, starting to incorporate new functionalities every time. However, the more resources are required for a system, the greater will be its complexity, the greater will be the number of available accesses and the bigger will be the difficulties to guarantee its security. Due to the fact, the computational environments became a frequent target of threats and attacks with a degree of increasing sophistication. This article supplies a general vision of the impacts of invasion on the computational systems, forthcoming its determinative and predisponent causes and describing the key element and benefits of a security politics based on the evaluation of risks and the integration of tools.

Keywords: Security; Integration; Threats; Attacks; Vulnerabilities.

[1] Especialista - Curso de Graduação Tecnológica em Redes de Computadores - UniFOA
jm.pinheiro@uol.com.br

1. Introdução

O inevitável desenvolvimento da Internet, aliado à necessidade cada vez maior de intercâmbio de informações forçou o estabelecimento de protocolos abertos de comunicação para prover conectividade e interoperabilidade entre diferentes plataformas, formando sistemas computacionais heterogêneos.

De acordo o CERT.br (2007), um computador (ou sistema computacional) é dito seguro se este atende a três requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade e disponibilidade. A confidencialidade indica que a informação está disponível apenas para aqueles indivíduos devidamente autorizados; a integridade, por sua vez, mostra que a informação não sofreu nenhuma alteração ou foi destruída e o sistema apresenta um desempenho satisfatório e, finalmente, a disponibilidade informa que os serviços e recursos do sistema estão disponíveis sempre que forem necessários.

Infelizmente, a popularização dos recursos de informática nos colocou frente a frente com problemas de segurança relacionados a ameaças, tentativas de ataques e invasões que afetam os requisitos básicos dos sistemas computacionais. Nesse enfoque, uma rede de computadores pode apresentar pontos susceptíveis a ataques, proporcionados pela má configuração do hardware ou software, administração equivocada dos recursos disponibilizados ou ambos. Boa parte dos recursos necessários para elevar o grau de segurança em uma organização já está disponível, mas são, geralmente, ignorados (MACHADO, 2007).

As vulnerabilidades dos sistemas computacionais podem ser agrupadas em três categorias principais: pessoais (omissão ou intenção criminal), de componentes (falha de equipamentos ou aplicativos) e de eventos (acidentes, fenômenos da natureza). Dentre esses tópicos, os aspectos pessoais, principalmente aqueles relacionados com a identificação e autenticação dos usuários no sistema são os itens mais visados. Por esse motivo, é fundamental reconhecer a importância do elemento humano nos ambientes computacionais, uma vez que o ser humano é invariavelmente o elo mais fraco da cadeia de segurança e sobre ele devem recair os principais cuidados durante as fases de especificação, implantação e gestão dos sistemas de segurança (Figura 1).

Figura 1 - Aspectos humanos são itens de vulnerabilidades dos sistemas

1.1. Ambiente Computacional

As camadas físicas e lógicas que compõem um sistema computacional estão interconectadas para atender às necessidades dos diversos usuários situados interna ou externamente a ele. Isso significa que as informações críticas residem em vários níveis na rede interna, onde cada qual requer sua própria proteção.

Enquanto a Tecnologia da Informação (TI) enfocava no passado uma segurança centralizada da base de dados, no presente, passou a lidar com a expansão do alcance das redes locais e com uma abrangência maior dos requisitos de segurança correspondentes. Ao mesmo tempo, as ameaças aos sistemas computacionais se tornaram mais sofisticadas e os atacantes passaram a empregar diversos meios de propagação, assim como se empenham em descobrir e explorar diferentes vulnerabilidades dos sistemas conectados em rede.

1.1.1. Ameaças

Uma ameaça consiste em uma possível violação do sistema computacional e pode ocorrer de forma acidental ou intencional. Uma ameaça acidental é aquela que não foi planejada; Pode ser causada por uma falha no hardware (defeito no disco rígido) ou no software (falha no sistema operacional, por exemplo). Já uma ameaça intencional, como o nome diz, está associada à intencionalidade premeditada. Pode se caracterizar pelo monitoramento não autorizado do sistema, até tentativas de exploração de eventuais falhas na configuração dos aplicativos.

De acordo com Moreira (2001):

Todos os ambientes computacionais são vulneráveis a incidentes de segurança e, portanto, à ação de ameaças. Alguns com maior, outros com menor probabilidade de ocorrência, devido ao grau de eficiência das medidas de segurança implementadas.

Dentre as principais ameaças aos sistemas computacionais estão aquelas que envolvem a destruição de informações e de recursos, a modificação ou deturpação da informação, roubo, remoção ou perda de informação ou funcionalidades, revelação de informações confidenciais, chegando até a interrupção de serviços de rede.

1.1.2. Ataques

Um ataque ocorre quando uma ameaça intencional se concretiza. Toda ameaça, quando concretizada, causa uma perda ou um dano a algum recurso (MOREIRA, 2001). Os ataques ocorrem por motivos diversos e variam entre a curiosidade, passando pelo interesse em adquirir conhecimento, pelo teste de capacidade "vamos ver se eu sou capaz", até o extremo, relativo a ganhos financeiros, extorsão, chantagem, espionagem industrial, venda de informações confidenciais e, o que está muito na moda, ferir a imagem de um governo ou uma determinada empresa ou serviço. A segurança não é um problema de tecnologia; é uma questão social. Tratando-a como um problema que pode ser resolvido por meios tecnológicos, você estará se expondo a um ataque (WADLOW, 2001).

Quando um ataque bem sucedido acontece, a notícia da invasão é proporcional à fama de quem a sofreu e normalmente representa um fato negativo em termos de repercussão pública.

1.2. Motivação para invasões

Qualquer tipo de invasão terá sempre um motivo determinado que impulsione o(s) atacante(s) ao(s) seu(s) objetivo(s) (motivação) e fatalmente passará por uma fase de planejamento criterioso (técnica), podendo levar algum tempo (oportunidade) até que se concretize (Figura 2).

Figura 2 - Fatores determinantes para a invasão de um sistema

Os fatos que motivam as invasões aos sistemas computacionais são diversos, entretanto, podem ser classificados dentro de seis grupos principais:

· Espionagem Industrial – visa ao roubo ou à destruição de informações sigilosas dos concorrentes;
· Benefício Próprio – ocorre quando existe a possibilidade de, ao invadir um sistema, o indivíduo obter vantagens financeiras e ou pessoais;
· Vingança – um usuário (ou ex-usuário) sentindo-se injustiçado promove alterações no sistema que podem causar sérios prejuízos;
· Status – um sistema computacional, razoavelmente seguro, representa um desafio para as comunidades de invasores. A necessidade de ser reconhecido faz com que o indivíduo tente invadir o sistema para atingir uma posição de destaque entre seus pares;
· Desafio – a invasão de sistemas importantes, em que a segurança está em um nível muito alto, torna-se uma aventura para os invasores, independente das informações obtidas;
· Maldade – A invasão e a destruição do sistema de informação pelo simples prazer de destruir.

2. Causas Determinantes e Predisponentes

Apesar da segurança dos sistemas computacionais não ser a competência básica da maioria das organizações, ela é claramente um requisito para a existência da própria organização. A segurança, então, se torna um fator-chave do negócio, não somente uma opção de TI. Entretanto, qualquer sistema pode apresentar vulnerabilidades que o deixam exposto a ameaças e ataques. O sucesso desse tipo de investida ocorre, muitas vezes, simplesmente porque os responsáveis pela administração dos sistemas não possuem o

treinamento adequado ou simplesmente negligenciam suas atribuições. Como agravante podem faltar ferramentas de gerenciamento eficientes para coibir essa prática pela falta de investimentos em segurança.

Segundo Oliveira (2001), a segurança de informações é um item complexo e pode abranger várias situações como: erro, displicência, ignorância do valor da informação, acesso indevido, roubo, fraude, sabotagem, causas da natureza, etc.

Normalmente, a invasão de um sistema se dá pela soma de vários fatores que, em conjunto, se potencializam e culminam com um ataque bem sucedido (Figura 3). Ao listar as possíveis causas envolvidas, pode-se chegar à conclusão da causa mais relevante. Essa é chamada de causa determinante. As demais causas, que possibilitaram o evento, são chamadas de causas predisponentes. Comumente se dá mais importância às causas predisponentes porque elas são variadas, em geral simples, podendo ser distribuídas entre vários responsáveis e, teoricamente, mais fáceis de resolver. Infelizmente esse procedimento apenas desvia a atenção da causa determinante, a verdadeira responsável pelo fato ocorrido.

Figura 3 - A invasão de um sistema normalmente se dá pela soma de vários fatores

2.1. Reconhecendo as verdadeiras causas de um ataque

Causas determinantes são criadas lentamente, passando a fazer parte da rotina e, por esse motivo, difíceis de serem percebidas. Em geral, são compensadas, por algum tempo, pelo controle das causas predisponentes conhecidas. Quando algumas dessas causas saem do controle, a causa determinante se sobrepõe e o ataque fatalmente ocorre. Por exemplo, pode-se afirmar que as causas que determinam o infarto são a genética, o colesterol e a pressão alta; o que predispõe são o cigarro, o estresse e o sedentarismo. De pouco adianta parar de fumar sem controlar a pressão alta.

O que pode determinar um ataque bem sucedido a um sistema computacional é o despreparo profissional, a ausência de uma política de segurança eficaz e a falta de investimentos; o que predispõe é a ausência de treinamento do pessoal, descaso com a segurança e ferramentas de gerenciamento eficientes.

Segundo Wadlow (2001):

> A segurança é um processo. Pode-se aplicar o processo seguidamente à rede e à empresa que a mantém e, dessa maneira, melhorar a segurança dos sistemas. Se não iniciar ou interromper a aplicação do processo, sua segurança será cada vez pior, à medida que surgirem novas ameaças e técnicas.

A invasão de um sistema computacional reúne uma série de causas predisponentes: ameaças por códigos maliciosos (vírus, cavalos de tróia, backdoors, etc), engenharia social, utilização incorreta dos recursos por desconhecimento ou até mesmo por má fé, dentre outras. A causa determinante poderá estar na imprevisão dos usuários, na irresponsabilidade ou falta de percepção dos administradores dos recursos ou pior, na omissão generalizada dos indivíduos envolvidos no processo.

2.2. Avaliação de Riscos

A avaliação de riscos representa um processo formal de identificação e priorização dos riscos e que oferece um direcionamento detalhado sobre a realização de avaliações das causas determinantes e predisponentes que podem levar a um ataque ao sistema computacional.

O processo de avaliação de riscos pode ser dividido em três etapas distintas:

· Planejamento – planejar a coleta de dados dos possíveis riscos utilizando um processo consistente e fácil de reproduzir;
· Coleta de dados – coletar os dados de risco através da análise da utilização do sistema, observando aspectos técnicos e humanos;
· Priorização de riscos – classificar e priorizar os riscos detectados segundo um critério de avaliação previamente estabelecido.

O planejamento adequado da avaliação de riscos é essencial para que o processo de identificação e priorização de riscos seja bem sucedido. Falhas na definição dos critérios de avaliação, a falta de alinhamento entre os participantes ou erros na definição do escopo das atividades podem comprometer a eficácia das etapas de coleta de dados e priorização de riscos.

A fase da coleta de dados deve abranger informações referentes aos ativos organizacionais com uma breve descrição de cada item, sua importância, os motivos ou eventos que podem afetá-lo negativamente, as vulnerabilidades conhecidas e uma descrição dos controles atuais e sua eficácia. Envolve também um levantamento quanto à situação dos usuários, nível de interação com o sistema e treinamento que cada um possui.

Na etapa final do processo de avaliação de riscos, as informações obtidas durante a coleta de dados devem ser organizadas. Entretanto, a priorização dos riscos tem natureza subjetiva, uma vez que envolve uma previsão para o futuro. O resultado é uma lista que fornece uma série de informações preliminares e que será o suporte para a tomada de decisões quanto à política de segurança que deverá ser adotada. Nesse momento é muito importante estabelecer um processo transparente com funções e responsabilidades bem definidas para que os resultados obtidos sejam reconhecidos e utilizados para a redução dos riscos através de investimentos conscientes na área de TI.

3. Política de Segurança

A Política de Segurança se preocupa com a aplicação das proteções (técnicas e administrativas) objetivando minimizar as possíveis vulnerabilidades e anular potenciais possibilidades de falhas, uma vez que a invasão de um sistema computacional dificilmente resulta de uma ameaça única.

Segundo Ferreira e Araújo (2006):

> A política de segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação devendo ser formalizada e divulgada a todos os usuários que fazem uso dos ativos de informação.

Essa política atribui responsabilidades e direitos aos indivíduos que lidam com os recursos computacionais e com as informações neles armazenados, definindo as atribuições de cada um em relação à segurança dos recursos com os quais trabalham, ditando o que pode ou não ser feito na rede e o que será considerado inaceitável.

Ferreira e Araújo (2006) afirmam:

> A política, preferencialmente, deve ser criada antes da ocorrência de problemas com a segurança, ou depois, para evitar reincidências. Ela é uma ferramenta tanto para prevenir problemas legais como para documentar a aderência ao processo de controle de qualidade.

Na política de segurança também são definidas as penalidades às quais estão sujeitos os usuários que não cumprirem as determinações dessa política. Trata-se, pois, de um mecanismo preventivo de proteção que define um padrão de segurança a ser seguido pelo pessoal técnico, pelo nível gerencial e os demais usuários (internos e externos) do sistema. Pode ser usada ainda para definir as interfaces entre usuários, fornecedores, parceiros e para medir a qualidade e a segurança dos sistemas atualmente em uso. Uma de suas preocupações é estabelecer os métodos de proteção, o controle e monitoramento dos recursos computacionais disponibilizados.

De acordo com Machado (2007):

> Investir em tecnologias para segurança não se resume a comprar um firewall, trazê-lo embaixo do braço e colocá-lo na sua rede. Caso sua configuração seja displicente, seria mais vantajoso vendê-lo e usar este dinheiro na recuperação de um ativo pós-incidente.

A política de segurança deve definir as responsabilidades das funções relacionadas à segurança e discriminar as principais ameaças, riscos e impactos envolvidos (Figura 4). Ela deve integrar-se às metas de negócio da organização e ao plano das políticas de informatização, influenciando todos os projetos de informatização tais como a utilização de novos sistemas, planos de contingência, planejamento de capacidade, dentre outros.

Figura 4 - A política de segurança define responsabilidades e penalidades no uso dos recursos computacionais

É importante salientar que a política de segurança não envolve apenas a área de Tecnologia da Informação, mas a organização como um todo; como toda política institucional, deve ser aprovada pela alta gerência e divulgada aos funcionários e demais usuários dos serviços computacionais.

Segundo Machado (2007), o incentivo para aumentar o nível de segurança deve começar por cima, com a disseminação de uma filosofia de comportamentos e atitudes que podem reduzir bastante a incidência de problemas no ambiente organizacional.

3.1. Soluções Integradas de Segurança

Devido à rápida evolução das ameaças e ataques, a segurança computacional é um alvo em constante movimento. Apesar de nenhum sistema de segurança ser absolutamente infalível, um sistema de várias camadas, suportado por políticas abrangentes de segurança pode reduzir significativamente o risco de ataques e invasões. Segundo a Symantec (2007), as soluções de segurança atuais são normalmente compostas de vários produtos, resultando em uma falta de interoperabilidade, gerenciamento e alto custo de propriedade.

As soluções de segurança usadas nas empresas consistem de vários produtos que, via de regra, são adquiridos, instalados, distribuídos, gerenciados e atualizados separadamente. Essas soluções, individualmente, podem ser incômodas para instalar e geralmente são difíceis e caras de gerenciar e atualizar, uma vez que o custo e os recursos necessários para esse fim aumentam consideravelmente (Figura 5). Outras implicações dessas soluções de segurança incluem resultados insatisfatórios, incompatibilidade entre produtos e um alto custo de propriedade.

Adicionalmente ao fornecimento inadequado de proteção às diversificadas ameaças, são muitos os produtos que requerem implementação e configuração através de um suporte especializado. Entretanto, quando integradas, elas podem oferecer uma proteção mais completa enquanto a complexidade e o custo são reduzidos.

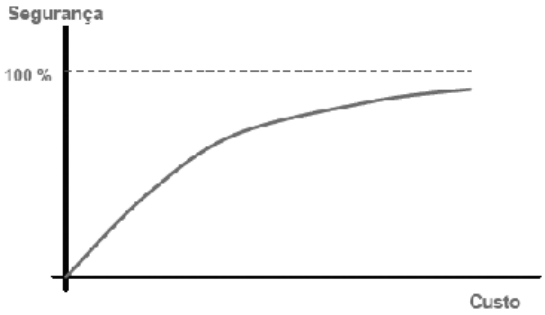

Figura 5 – O custo da segurança cresce com o aumento do número de soluções utilizadas

Uma abordagem de segurança integrada oferece a postura de segurança mais efetiva no raio máximo de custo-benefício, comparado às implementações de segurança de vários produtos (SYMANTEC, 2007).

Partindo dessa premissa, uma solução de segurança integrada fornece um sistema holístico e completo, capaz de combinar diferentes tecnologias com compatibilidade de política de segurança, gerenciamento, serviços, suporte e pesquisa avançada para a proteção completa do sistema computacional, além de permitir a realocação do pessoal de TI para outros projetos estratégicos, melhorando o gerenciamento de segurança de forma geral. Por outro lado, através da combinação de várias funções, uma solução de segurança integrada será capaz de proteger o sistema com mais eficiência contra uma variedade maior de ameaças e minimizar os efeitos dos ataques que venham a ocorrer.

4. Conclusões

Assim como um sistema computacional absolutamente seguro ainda não existe, a segurança não pode ser encarada como uma questão apenas técnica,

mas que envolve também aspectos gerenciais e humanos. Não adianta adquirir uma série de dispositivos de hardware e software sem treinar e conscientizar todos os indivíduos que os utilizam.

Outra grande dificuldade está no fato de que, na mesma proporção, ou até mesmo com maior intensidade com que buscamos assegurar as nossas comunicações e informações, o conhecimento, as ferramentas e as técnicas disponíveis aos agressores também têm se aprimorado. Não importa quão seguro se faça um sistema computacional, sua segurança sempre estará em risco se houver motivação, técnica e oportunidade suficientes para um ataque.

As técnicas e tecnologias atuais de segurança vêm atingindo suas limitações, sendo necessárias soluções inovadoras para lidar com o nível dos ataques e das ameaças atuais e futuras. Uma nova estratégia de segurança baseada na integração e uniformidade das soluções pode permitir a melhoria da postura de segurança geral do sistema de uma forma que não seria possível atingir através de uma implementação de produtos individuais, segundo padrões conservadores. Ao aplicar uma abordagem integrada aos sistemas e aos dispositivos, pode-se garantir a atualização uniforme dos aspectos críticos da segurança computacional independente de onde e como os recursos estejam alocados.

5. Referências

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.br. Cartilha de Segurança para Internet 3.1. Disponível em: http://cartilha.cert.br/. Acesso em jun 07.

FERREIRA, F. N. F. e ARAÚJO, M. T. *Política de Segurança da Informação: Guia Prático para Elaboração e Implementação.* Rio de Janeiro: Ciência Moderna, 2006.

MACHADO, M. *Uso correto dos Recursos de Segurança.* Disponível em: http://www.modulo.com.br/arquivoboletins/arqblt_2002.jsp. Acesso em jun 07.

MOREIRA, N. C. *Segurança Mínima: Uma visão corporativa da Segurança de Informações.* Rio de Janeiro: Axcel Books, 2001.

OLIVIERA, W. J. *Segurança da Informação: Técnicas e Soluções*. Florianópolis: Visual Books, 2001.

SYMANTEC. *Segurança Integrada: Criando uma empresa segura.* Disponível em: http://www.symantec.com/region/br/msn/downloads/apostilas/. Acesso em ago 07.

WADLOW, T. A. *Segurança de Redes: Projeto e gerenciamento de redes seguras.* Rio de Janeiro: Campus, 2001.

Informações bibliográficas:
Conforme a NBR 6023:2002 da Associação Brasileira de Normas Técnicas (ABNT), este texto científico publicado em periódico eletrônico deve ser citado da seguinte forma:
PINHEIRO, J. M. S.. Os Benefícios da Política de Segurança Baseada na Avaliação de Riscos e na Integração de Ferramentas. Cadernos UniFOA , Volta Redonda, ano II, n. 4, agosto. 2007. Disponível em: <http://www.unifoa.edu.br/pesquisa/caderno/edicao/04/28.pdf>