SEGURANÇA DA INFORMAÇÃO: um estudo a partir dos Crimes Virtuais

Gecileia Aparecida Caetano[1]
Prof.Ms Marta Alves de Souza[2]
Prof.Ms Helder Rodrigues Costa[3]

RESUMO

Este estudo procura compreender até que ponto os sistemas de segurança, nomeadamente voltados para crimes virtuais (como ataques às Instituições financeiras, clonagem de cartão de crédito, falsidade ideológica, roubo de dados) estão preparados para proteger as informações dos constantes ataques ocorridos na rede. Os recursos tecnológicos têm sido um grande atrativo para as práticas criminais, facilmente explorados pela rapidez, facilidade e economia com que certas ações podem ser executadas. Embora os sistemas de detecção de intrusos garantam uma maior prevenção, eles sozinhos, não são plenamente eficientes para sanar todos os problemas de segurança. Vale ressaltar que apesar do IDS ser uma ferramenta destinada à segurança de rede, ele é apenas um componente em uma solução de segurança e também está sujeito a falhas. Assim, conclui-se que o IDS deve ser usado em conjunto com diversas outras medidas de segurança, pois o sistema de detecção de intrusos é eficiente, mas não atende plenamente a segurança das organizações. Por isso, em decorrência da evolução das técnicas utilizadas nos crimes virtuais, os IDS necessitam de constantes pesquisas e evoluções no campo da segurança.

Palavras-chaves**:** intruso; Firewall; IDS; segurança da informação; crime virtual.

Abstract

This study it looks for to understand until point the security system, nominated come back toward virtual crimes as attacks to the financial Institutions, clone of credit card, false representation, robbery of data is prepared to protect the information of the constant attacks occurred in the net. The technological resources have been great a attractive one for practical the criminal ones, easily explored for the rapidity, easiness and economy with that certain actions can be executed. Although the detection systems of intruder guarantee a bigger prevention, them they are inefficacious for the security of the information, therefore, exist some attacks that the IDS do not obtain to detect, as the internal attacks, in the case of badly intentioned employees, the IDS does not guarantee much protection. In this context, it is necessary to adopt a set of methodology, being prevented to make static use of firewall. Thus, it is concluded

[1] Tecnólogo em Processamento de Dados – gelekaa@hotmail.com

[2]Mestre em Administração e Planejamento de Sistemas de Informação(PUCCAMP).Especialista em Informática em Educação (UFLA). profmarta@gmail.com

[3] Mestre em Ciências e Técnicas Nucleares pela Universidade Federal de Minas Gerais – UFMG. Bacharel em Engenharia Elétrica (UFMG).Coordenador do Curso de Gestão em Tecnologia da Informação – SENAC – MG.

that the IDS must be used in set with diverse other measures of security, therefore the detection system of intruder is efficient, but the security guard of the organizations does not take care of. Therefore, in result of the virtual crimes, the IDS need constant research in the field of the security.

Key-words: intrusion; Firewall; IDS; security of the information; virtual crime.

1 INTRODUÇÃO

Nas últimas décadas, a vida diária encontra-se cada vez mais em um mundo digitalizado. Com a popularização da internet e o crescimento do comércio eletrônico, a segurança de dados tem sido uma preocupação constante para as empresas que oferecem serviços na rede virtual. Neste novo meio virtual é possível estudar, trabalhar, casar, investir em recursos financeiros, vender, praticar atos de vandalismo, inclusive praticar crimes.

Com a expansão das redes sociais (Orkut, Facebook, Twiter entre outras) tão presentes no dia a dia das pessoas, é muito importante saber identificar e distinguir o que é seguro e o que pode ser utilizado para praticar crimes na internet. A rede virtual revela evidências de que os criminosos estão se utilizando de sofisticados mecanismos tecnológicos para atingir a sociedade e as organizações. Essas falhas na segurança têm atingido o mundo globalizado, a sociedade em geral, que se encontra cada vez mais dependente das máquinas e da internet. Tais ameaças têm comprometido a segurança da informação e o sucesso de muitas empresas, pois, à medida que estas se expandem, é cada vez mais importante descobrir quais são os pontos vulneráveis e, a partir deles, avaliar os impactos e riscos causados às mesmas.

Neste contexto, até que ponto os sistemas de segurança, especificamente os sistemas de detecção de intrusos, voltados para proteção contra crimes virtuais (como ataques às Instituições financeiras, clonagem de cartão de crédito, falsidade ideológica e roubo de dados) estão preparados para proteger as informações dos constantes ataques ocorridos na rede?

Sendo assim, trabalha-se com a hipótese de que os sistemas de segurança atendem de forma eficiente a determinadas demandas, mas sua proteção não é

absoluta, uma vez que os mesmos não evoluem na mesma velocidade que os crimes praticados por meio da internet.

Nesse sentido, o objetivo geral deste estudo é compreender até que ponto os sistemas de segurança, nomeadamente voltados para proteção contra crimes virtuais (como ataques às Instituições financeiras, clonagem de cartão de crédito, falsidade ideológica, roubo de dados) estão preparados para proteger as informações dos constantes ataques ocorridos na rede. Especificamente, pretende-se descrever os crimes executados na internet, bem como identificar as principais ações de prevenção e combate adotadas pelo governo e empresas da iniciativa privada.

2 REFERENCIAL TEÓRICO

2.1 Segurança da Informação (SI)

A segurança da informação é a proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação não-autorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (NBR 17999, 2003; DIAS, 2000; WADLOW, 2000; KRAUSE; TIPTON, 1999).

SI é manter as informações protegidas de acordo com as perspectivas e necessidades do usuário, ou seja, tê-las onde e quando precisar de forma confiável e correta, como também, mantê-las fora do alcance de pessoas não autorizadas. Na atual era da informação, muitas empresas têm como principal ativo a própria informação, por isso, ela deve ser protegida por uma política de segurança.

Segundo ABNT (2005), em sua NBR 17799, a SI é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados,

analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e os requisitos de segurança de uma organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

Segurança é a base para dar às empresas a possibilidade e a liberdade necessária para a criação de novas oportunidades de negócio. É evidente que os negócios estão cada vez mais dependentes das tecnologias e estas precisam estar de tal forma a proporcionar confidencialidade, integridade e disponibilidade – que conforme (NBR 17799, 2003; KRAUSE; TIPTON, 1999), são os princípios básicos para garantir a segurança da informação – das informações:

Confidencialidade – A informação somente pode ser acessada por pessoas explicitamente autorizadas; É a proteção de sistemas de informação para impedir que pessoas não autorizadas tenham acesso ao mesmo. O aspecto mais importante deste item é garantir a identificação e autenticação das partes envolvidas.

Disponibilidade – A informação ou sistema de computador deve estar disponível no momento em que a mesma for necessária;

Integridade – A informação deve ser retornada em sua forma original no momento em que foi armazenada; É a proteção dos dados ou informações contra modificações intencionais ou acidentais não-autorizadas.

Nakamura; Geus (2007, p. 21) “observam que a segurança significa permitir que as organizações busquem seus lucros, os quais são conseguidos por meio de novas oportunidades de negócios, que são resultado da flexibilidade, facilidade e disponibilidade dos recursos de informática. Portanto, a segurança deve ser considerada não apenas uma proteção, mas o elemento habilitador dos negócios da organização. De fato, pesquisas indicam que os consumidores deixam de realizar negócios via Internet quando não confiam na segurança de um site.”

Segundo Kurose (2006), uma das maneiras mais eficazes de garantir que as pessoas de má índole não causem danos, é assegurar, antes de mais nada, que suas tentativas de ataques e invasões sejam barradas antes de entrarem na rede.

Para tanto, o autor sugere que se utilize um dispositivo de segurança denominado firewall, que visa proteger a rede local do resto da internet.

Firewall é um sistema ou conjunto de sistemas que reforçam a política de segurança na comunicação entre redes com níveis de segurança diferentes.

Segundo Chapman (2000), "O Firewall é um componente ou conjunto de componentes que restringe o acesso entre uma rede protegida e a internet, ou entre outros conjuntos de rede."

O firewall controla o acesso à rede, regulando quais pacotes podem trafegar para dentro e para fora da rede. Desta forma, os princípios de uma comunicação segura concentra-se primordialmente em proteger a comunicação e recursos da rede, envolvendo também a detecção de falhas e ataques à infraestrutura e também a reação a esses ataques.

2.2 Sistemas de Detecção de Intrusos (IDS)

Sistema de Detecção de Intrusão, em inglês, *Intrusion detection system* (IDS), é um conjunto de meios técnicos para descobrir, em uma rede de computadores acesso não autorizado. Na verdade, são softwares que envolvem diversas técnicas e criam uma base de ações dentro da rede que pretendem detectar se algo saiu do padrão, ou seja, identificar máquinas que funcionam de forma diferente do padrão normal. O IDS auxilia na verificação do funcionamento da rede e ajuda os firewalls a serem mais eficientes, fornecendo subsídios e informações para que os firewalls tomem determinadas ações e também os servidores de Proxy trabalhem de forma integrada.

> **a) proxy:** sistemas que atuam como um *gateway* entre duas redes, permitindo as requisições dos usuários internos e as respostas dessas requisições, de acordo com a política de segurança definida (NAKAMURA; GEUS, 2007, p. 111).
> **b) firewall**: é um conjunto de componentes e funcionalidades que definem a arquitetura de segurança, utilizando uma ou mais tecnologias de filtragem (NAKAMURA; GEUS, 2007, p. 207, grifo do autor).

Nakamura; Geus (2007) "definem que IDS tem como objetivo detectar atividades suspeitas, impróprias, incorretas ou anômalas. Trata-se um elemento importante dentro do arsenal de defesa da organização. Além de ser crucial para a

segurança interna, o IDS pode detectar ataques que são realizados por meio de portas legítimas permitidas e que, portanto, não podem ser protegidos por alguns tipos de firewall. O mesmo ocorre quando um modem é utilizado sem autorização por um usuário interno. Tentativas de ataques contra qualquer recurso da organização também podem ser detectadas, mesmo que elas sejam normalmente barradas pelo firewall".

Ainda os mesmos autores advertem que: "o IDS trabalha como uma câmera ou um alarme contra as intrusões, podendo realizar a detecção com base em algum tipo de conhecimento, como assinaturas de ataques, ou em desvios de comportamento" (NAKAMURA; GEUS, 2007, p. 133).

Assim, o intruso é um invasor, um personagem que entra numa comunidade ou grupo sem permissão e a Intrusão é o conjunto de ações que tentam comprometer a tríade da segurança: integridade, confiabilidade e disponibilidade dos dados e ou sistema. A intrusão tenta burlar a cadeia de segurança mantida dentro da rede, fazendo com que a mesma pare. O sistema passa a trabalhar de forma indesejada, e até mesmo pode ser interrompido.

Outro aspecto que se deve observar é a distinção entre ataques provenientes do meio externo e os ataques originados a partir do mau uso do sistema, que são aqueles originários do meio interno. Estes ataques muitas vezes têm origem dentro da própria empresa, nem sempre estes são de procedência externa. Um indivíduo com acesso em sua casa pode fazer muito mais coisas do que outro de fora.

Afinal, colaboradores internos conhecem bem a topologia da rede e quais são os recursos de segurança disponíveis, além de saber onde os dados sensíveis estão armazenados.

A intrusão por mau uso do sistema ocorre quando pontos fracos são atacados seguindo padrões bem definidos. Este tipo de ataque pode ser descoberto através de monitoramento de certas ações realizadas em determinados objetos, comparando os padrões junto aos dados colhidos na auditoria dos sistemas.

Já na intrusão devido a mudança de padrão (anomalia), pode-se detectar a alteração de comportamento em relação ao uso normal do sistema através de valores que são apurados a partir de parâmetros do sistema.

Considerando o fato de que a maioria dos recursos de segurança é direcionada para proteger os ativos das empresas de ataques externos, muitos ataques podem não ser detectados, ou, quando o são, pode ser tarde demais. Sendo assim, são necessários mecanismos tecnológicos, tanto de hardware e principalmente de software que detecte os dois tipos de ataque: externos ou internos. Um sistema de IDS eficiente deve detectar tais ataques, (internos/externos), permitindo desta forma que o administrador de segurança tenha conhecimento sobre o que está acontecendo e sobre qual medida tomar com relação ao ataque, sempre de acordo com a política de segurança da empresa.

No tocante à categoria dos sistemas de detecção de intrusos tem-se, a saber: a) o Knowledge-Based Intrusion Detection, também conhecido como Misuse Detection System. Esse tipo de IDS tira proveito de falhas publicamente conhecidas no sistema, ou seja, faz o acesso indevido ao sistema através de falhas já conhecidas; b) Behavior-Based Intrusion Detection, também conhecido como *Anomaly Detection System*. Este outro, procura desvios na utilização normal do sistema, força o sistema a responder de forma inadequada.

Conforme Nakamura; Geus (2007, p. 143) “o *protocol Anomaly Detection-Based* é um tipo de IDS com base em comportamento é baseado em anomalia de protocolo, faz a análise do fluxo de pacotes para identificar irregularidades e inconsistências com relação aos padrões específicos de cada protocolo. Com o objetivo de identificar tráfego que viola especificações-padrão, como as Request for Comments (RFC), atividades suspeitas, como um ataque de buffer overflow”.

2.3 Tipos De IDS

De acordo com Nakamura; Geus (2007), há três tipos de sistemas de detecção de intrusão, a saber: 1) *Host-Based Intrusion Detection System* (HIDS) monitora os eventos e *logs* ou atuam como agentes de auditoria em um computador

ou servidor, ou seja, atuam localmente analisando os eventos de apenas um computador; 2) *Network-Based Intrusion Detection System* (NIDS) monitora o tráfego da rede, procura por padrões que possam representar um ataque, trabalhando dentro de uma rede local; e 3) IDS híbrido (Hybrid IDS) o processo evolutivo que acontece com toda tecnologia levou ao desenvolvimento do IDS híbrido (Hybrid IDS), que aproveita as melhores características do HIDS e do NIDS. 4)*Wireless Instrusion Detection System* (WIDS) é semelhante a um NIDS, porém, voltada para redes sem fio.

Nakamura; Geus (2007) discutindo os três primeiros tipos de sistemas de detecção de intrusão ou de intrusos verificam que Host-Based Intrusion Detection System (HIDS) funciona em cada sistema e é capaz de detectar intrusões com base em registros e eventos do sistema. Já o Network-Based Intrusion Detection System (NIDS) trabalha capturando pacotes da rede e realizando a análise de acordo com padrões ou assinaturas conhecidos. O IDS híbrido (Hybrid IDS) incorpora características do NIDS e do HIDS, de modo a oferecer uma capacidade maior de detecção. O IDS híbrido (Hybrid IDS) tem como objetivo combinar os pontos fortes do HIDS e do NIDS, a fim de oferecer uma melhor capacidade de detecção de intrusões. O IDS híbrido opera como um NIDS, coletando o tráfego da rede, processando os pacotes e detectando e respondendo a ataques e interage com seus agentes (HIDS) que atuam nos servidores/sistemas mais críticos da rede de uma empresa.

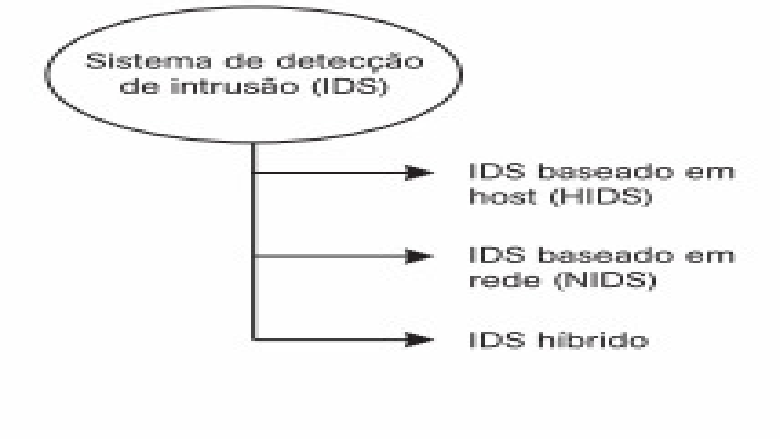

Figura 1 – Tipos de IDS
Fonte: Nakamura; Geus (2007, p. 256)

A Figura 1 mostra o Sistema de detecção de intrusos (IDS) e suas três categorias.

Devido à grande variedade de IDS, surgiu um conjunto de componentes chamado CIDF (*Common Intrusion Detection Framework)* com o objetivo de compreender os tipos, o funcionamento e as razões de IDS em uma rede. Este agrupa uma variedade de elemento que define uma ferramenta de IDS. Existem diferentes IDSs baseados em diferentes frameworks conceituais, no entanto, é possível identificar uma arquitetura comum. Terminologia introduzida pelo grupo de trabalho CIDF (Common Intrusion Detection Framework), event boxes (E-boxes) gera eventos utilizando dados de auditoria do sistema. Analysis boxes (A-boxes) analisa os eventos produzidos pelo E-boxes ou em alguns casos outros A-boxes, gerando alertas (ou alarmes). Database boxes (D-boxes) armazenam eventos e/ou alertas permitindo uma análise postmortem. Response boxes (R-boxes) disparam a reação a um ataque detectado.

2.4 Crimes Virtuais

2.4.1 Ataques às Instituições Financeiras e Clonagem de Cartão de Crédito

Conforme Terceiro (2011), dentre os delitos perpetrados pelos criminosos virtuais, podemos citar as constantes investidas as contas bancárias alheias, desviando seus valores para contas fantasmas de amigos ou próprias e, nessa mesma linha de delitos um dos mais usuais delitos dessa natureza que é a "invasão" de computadores particulares com o intuito de ler os chamados e-mails.

Segundo Braun (2011), atualmente, há uma média de 100 a 150 quadrilhas especializadas em fraudes eletrônicas atuando no País. Com o projeto Pentáculo, em parceria com bancos privados, a Polícia Federal conta com um banco de dados de todas as fraudes em internet banking e clonagem de cartões no País .

Pesquisa da eMarketer, empresa norte-americana especializada em estudos sobre a internet, aponta que o Brasil está em segundo lugar na lista de ataques sofridos, no ano passado, com 5.568, incluindo fraudes, roubos, brechas de segurança e interrupção de serviços. Os Estados Unidos lidera a estatística, com

26.792 ocorrências. Na maioria das vezes os próprios usuários, por falta de informações, são infectados e prejudicados financeiramente ou moralmente por isso.

Segundo Techlider (2011), Brasil lidera o número de tentativas de roubo de dados bancários pela Internet na América Latina, é o que diz a ESET, empresa européia de segurança digital que conta com um laboratório de ameaças localizadas na região.

2.4.2 Falsidade Ideológica

Segundo a Wikipedia (2011) Falsidade ideológica - é um tipo de fraude criminosa que consiste na adulteração de documento, público ou particular, com o fito de obter vantagem - para si ou para outrem - ou mesmo para prejudicar terceiro. Ocorre quando alguém mente seu nome, idade, estado civil, sexo e outras características com o objetivo de obter alguma vantagem ou prejudicar outra pessoa. Pode acontecer numa rede social, por exemplo, se um adulto mentir de má fé e se fizer passar por um adolescente para se relacionar com estes usuários.

2.4.3 Roubo de Dados

Segundo a Safernet (2011) Roubo de dados – é o tipo de ataque cometido através dos meios virtuais contra uma rede on-line, no intuito de abstrair informações alheias, ou seja, assumir e/ou tomar pose dos dados pessoais de alguém ou de alguma organização, como perfil, senha, avatar, e-mail sem a autorização ou concordância destes, para qualquer fim com o intuito de práticas ilícitas consideradas como crime.

2.4.4 IDS e os Crimes Virtuais

Conforme Nakamura; Geus (2007, p. 133) o IDS é um elemento importante dentro do arsenal de defesa da organização. Além de ser crucial para a segurança interna, pode detectar ataques que são realizados por meio de portas legítimas permitidas e que, portanto, não podem ser protegidos pelo firewall. O IDS é capaz de detectar e alertar os administradores quanto a possíveis ataques ou comportamentos anormais na organização. Eles podem oferecer subsídios suficientes para que a organização melhore sua proteção contra quaisquer tipos de ataque, principalmente os considerados internos.

Diante de todo o arsenal de defesa disponíveis e utilizados nas organizações, ainda assim, a lista dos crimes perpetrados através dos meios eletrônicos é extensa e essa prática tem aumentado com a universalização da internet, o crescimento das redes sociais e programas de mensagens instantâneas, e-commerce, serviços bancários dentre outros serviços ofertados e perante a facilidade cada vez maior de acesso à rede, maior também, é a exposição dos internautas e a vulnerabilidade aos crimes virtuais.

Contrário às benesses que a internet oferece, existem também constantes tentativas de exploração maliciosa das informações, tornando-se imprescindível o zelo e a preocupação pela segurança. Investir num bom software de antivírus e mantê-lo diariamente atualizado é a uma dentre as importantes medidas de combate. Porém, em termos de segurança não se pode negligenciar as atualizações. É imprescindível investir também num firewall, e principalmente adotar uma política de segurança eficiente. Nas empresas, independentemente de tamanho, a rede costuma estar conectada à internet o tempo todo. Se isso significa mais agilidade no atendimento aos clientes e na resolução de problemas, também é verdade que expõe o sistema a ataques maliciosos. Cabe ressaltar aqui, que a conscientização do usuário sobre o uso adequado da internet e os cuidados que se deve ter ao acessar determinados serviços e conteúdos disponíveis na rede, é parte integrante da prevenção.

Nakamura; Geus (2007). “Um dos objetivos do IDS é detectar se alguém está tentando entrar no seu sistema ou se algum usuário legítimo esta fazendo uso

inadequado do mesmo. Ao detectar algo suspeito ou ilegal, ele gera uma notificação. Isso se dá diante de qualquer anomalia do sistema como também de seus usuários.

A utilização de um IDS, resolve parte dos problemas, porém, faz-se necessário usar outros recursos de segurança em conjunto com os sistemas de detecção de intrusão verificando os pontos importantes da rede, e avaliando a necessidade da instalação de um IDS, levando em consideração alguns aspectos expressivos, como servidores, protocolos, conexões externas, serviços, mecanismos de proteção que já foram implementados, entre outros".

Ao se constatar um ataque a um sistema, o IDS não utiliza medidas preventivas, e sim age como um informante, alertando o administrador do sistema sobre o que está ocorrendo. Uma das maneiras mais comumente usadas para descobrir instrusões é a utilização de dados das auditorias gerados pelos sistemas operacionais, cujos acontecimentos ordenados cronologicamente, sendo possível a inspeção manual destes registros, o que não é uma prática viável, uma vez que estes arquivos de logs apresentam tamanhos consideravelmente grades. Com o IDS, a tarefa de analisar estes dados colhidos com a auditoria é automatizada, sendo isto de extrema utilidade, pois os dados podem ser usados a fim de estabelecer a culpabilidade do atacante e na maioria das vezes, pode ser o único modo de descobrir uma atividade sem autorização, detectar a extensão dos dados e prevenir tal ataque no futuro, tornando desta forma o IDS uma ferramenta extremamente valiosa para análises em tempo real e também após a ocorrência de ataque (MELO, 2002)

3 METODOLOGIA

Foi realizada uma pesquisa baseada em artigos científicos, livros e sites da internet. Nesse caso, tratou-se de uma pesquisa classificada quanto aos objetivos como explicativa, valendo-se do procedimento da pesquisa bibliográfica. De acordo com Antônio Carlos Gil, "essas pesquisas têm como preocupação central identificar os fatores que determinam ou que contribuem para a ocorrência dos fenômenos. Esse é o tipo de pesquisa que mais aprofunda o conhecimento da realidade, porque explica a razão, o porquê das coisas" (1994, p. 46).

Para sintetizar a característica da pesquisa bibliográfica, temos a definição de Santos:

> "pesquisa bibliográfica é a atividade de localização e consulta de fontes diversas de informações escritas, para coletar dados gerais ou específicos a respeito de um tema". (SANTOS, 2011, p.01).

4 CONSIDERAÇÕES FINAIS E SUGESTÕES

Neste ponto, é preciso voltar às questões colocadas no início do trabalho e resgatarmos os principais argumentos discutidos ao longo do mesmo.

Este estudo procurou explicar até que ponto os sistemas de segurança, nomeadamente voltados para proteção contra crimes virtuais (como ataques às Instituições financeiras, clonagem de cartão de crédito, falsidade ideológica, roubo de dados) estão preparados para proteger as informações dos constantes ataques ocorridos na rede.

Na análise desenvolvida, identificou-se que os recursos tecnológicos têm sido um grande atrativo para as práticas criminais, facilmente explorados pela rapidez, facilidade e economia com que certas ações podem ser executadas.

No tocante à eficácia de um servidor IDS, este sozinho, não é plenamente eficiente para sanar todos os problemas de segurança. Vale ressaltar que apesar do IDS ser uma ferramenta destinada à segurança de rede, ele é apenas um componente em uma solução de segurança e também está sujeito a falhas. Impossível imaginar segurança de rede, sem a implantação de um trabalho contínuo de avaliação e melhoria das ferramentas e atualizações/correções dos softwares, como também estar sempre atento às vulnerabilidades identificadas.

Uma política de segurança é o principal elemento para a segurança de qualquer organização. Enfim, adotar um conjunto de metodologias, evitando fazer uso de firewall estático, ou seja, bloquear serviços corriqueiros como MSN, Youtube entre outros, o IDS veio para que se possa fazer uma gerencia de segurança proativa, ou seja, baseada em fatos ocorridos em resultados, e não em fatos supostos, gerenciando de forma otimizada os ativos da organização. Os sistemas de detecção de intrusão devem ser ferramentas para a implementação de uma política

de segurança efetiva, mas, se utilizados isoladamente não serão uma solução definitiva para segurança das redes corporativas. O IDS deve ser usado em conjunto com diversas outras medidas de segurança.

Ante o exposto, foi possível verificar que a eficiência de um sistema de detecção de intrusão deve ser avaliada em conjunto com as ferramentas e tecnologias implementadas e que estes atendem ao que se propõem, mas sozinhos não solucionam o problema de segurança das organizações. Evidenciou-se também que em decorrência da evolução dos crimes virtuais, os IDS's necessitam de constantes pesquisas no campo da segurança.

REFERÊNCIAS

ANALISTA TI. Navegue protegido. Disponível em: <http://analistati.com/navegue-protegido/>. Acesso em: 6 jun. 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 17799: Tecnologia da Informação: Código de prática para a gestão da segurança da informação, elaboração. Rio de Janeiro: ABNT, 2005. 9 p.

BRAUN, Daniela. Segurança. Ataques e ameaças.**IDG now !**, Disponível em: <http://idgnow.uol.com.br/seguranca/2009/12/14/policia-federal-vai-investigar-90-dos-criminosos-digitais-ate-2011/>. Acesso em 01 de jun. 2011.

Chapman, D. B.; Zwicky, E. D. **Building Internet Firewalls**. Sebastopol, CA: O`Reilly & Associates, 1995.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. AxcelBooks. Rio de Janeiro, 2000

GIL, Antônio Carlos. **Como Elaborar um Projeto de Pesquisa.** 3ª ed., São Paulo, Atlas. 1994.

KRAUSE, Micki e TIPTON, Harold F.**Handbook of Information SecurityManagement**. Auerbach Publications, 1999.

MELO, L. Et al. (2002) **Implementação de IDS Open Source**. Universidade Católica de Brasília, Brasília. Dissertação

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais. **Jus Navigandi**, Teresina, ano 7, n. 58, 1 ago. 2002. Disponível em**:** <http://jus.uol.com.br/revista/texto/3186**>**. Acesso em**:** 6 jun. 2011**.**

SAFERNET. Roubo de dados Disponível em <:http://www.safernet.org.br/site/prevencao/cartilha/safer-dicas/roubo. Acesso em: 3 jun. 2011.

SANTOS, Eniel do Espírito. **Pesquisa Bibliográfica – Metodologia do Estudo e da Pesquisa**. Disponível em: http://www.heliorocha.com.br/.../MEP/MEP_Pesquisabibliografica.doc Acesso em: junho, 2011.

TECHILDER. Phishing faz o Brasil liderar ranking de ataques aos dados bancários: <http://www.techlider.com.br/2011/04/phishing-faz-o-brasil-liderar-ranking-de-ataques-aos-dados-bancarios/>. Acesso em: 03 de jun de 2011.

WADLOW, Thomas. **Segurança de Redes**. Editora Campus. Rio de Janeiro, 2000.

WIKIPEDIA. Falsidade ideológica. Disponível em: <http://pt.wikipedia.org/wiki/Falsidade_ideol%C3%B3gica/>. Acesso em: 4 jun. 2011.