PROJETO DE UMA CLASSIFICAÇÃO DE TRÁFEGO HOSTIL EM REDES DE COMPUTADORES[1]

PROJECT OF A CLASSIFICATION OF HOSTILE TRAFFIC ON COMPUTER NETWORKS

Patryck Ramos Martins

Secretaria de Estado da Saúde de Santa Catarina
E-mail: patryckrm@gmail.com

Rafael da Rosa Righi

SENAIsc Florianópolis
E-mail: righi@ctai.senai.br

Resumo. As hostilidades representam um agravante padrão em ambientes computacionais. Os desafios para identificar estes males digitais são constantes perante os pesquisadores. Encontrar o biótipo ideal de sistemas de defesa para combatê-las parece o cerne da solução aplicado por diversas organizações e profissionais de segurança, desprezando a individualidade do âmbito computacional combalido. Este documento define um novo prisma ao tratar e classificar tráfego hostil em redes de computadores, e busca com isso aprimorar o aprendizado sobre cada investida hostil contra sistemas computacionais. O projeto de uma classificação de tráfego hostil em redes de computadores chama-se CLATH. Ele mapeia atos hostis e prepara a organização qualificando o tráfego de dados maléficos de seu domínio. Dentre os pontos fortes desta abordagem, salienta-se a obtenção do nível de segurança de uma organização, índice que pode ser utilizado para acompanhar a evolução da segurança no cenário de rede.

Palavras-chave: Segurança computacional; Caracterização de tráfego; Gerência de redes

Abstract. *Hostilities represent a standard aggravating in computational environments. The challenges for identifying these digital evils are extensive for researchers. To find the ideal biotype of defense systems to fight them seems the core of the solution applied by various organizations and professionals of security, disdaining the individuality of the weakened computational scope. This document defines a new prism while treating and classifying hostile traffic in computer networks, and try with this to accomplish the learning on each hostile onslaught against computational systems. Therefore was created the CLATH, a project of classification of hostile traffic on networks of computers, which maps hostile acts and prepares the organization qualifying the traffic of malicious data of its domain. It is based on flowcharts and calculations of hostile indexes, which allow the individual characterization of each hostility, helping to find a final level of the security for the organization.*

Keywords: Computer security; Characterization of traffic; Network management

1 INTRODUÇÃO

O avanço constante de pesquisas sobre hostilidades tecnológicas por atacantes e pesquisadores seja, para o aproveitamento fortuito ou necessidade de buscar correções impele o fator segurança no âmbito organizacional. Como constatado em Cert (2007) e Cert.BR (2007) visualiza-se o aumento contínuo das hostilidades encontradas, que acercam os sistemas computacionais contribuindo para a degradação das tecnologias que sustentam organizações e ratificando a preocupação crescente sobre a segurança dos dados.

Apesar de todo o aparato tecnológico disponível para as organizações, projetar ambientes de rede seguros é uma prática complexa e com inúmeros detalhes, sendo um atributo complexo de implementar consistentemente em sistemas computacionais (CAMPELLO, SERAFIM e WEBER, 2002). Tendo em vista a prática de premissas duvidosas e processos implantados por tentativa e erro, conclui-se a mínima existência de metodologias comprovadas, padronizadas e difundidas na área de gerenciamento de segurança de redes (BARBATO et al, 2005; KIM e WARMACK, 2005). Diferentes institutos de pesquisas, como afirmam Brandão, Martimiano e Moreira (2004) e Papadaki *et al* (2002), têm realizado esforços no sentido de catalogar e classificar dados referentes à segurança computacional, mas percebem apesar dos avanços, dificuldades em estabelecer um vocabulário e classificação única.

No entendimento e classificação dos dados que tramitam em um ambiente de rede de computadores diferenciar o que é útil ou não é de suma importância para uma organização. Ao não ter a unificação destas informações sobre vulnerabilidades, ameaças e outros incidentes de segurança, um gestor pode absorver informações incertas sobre o tráfego de dados de seu domínio. Logo, não basta a implantação de tecnologias de segurança como sistemas *Intrusion Detection System (IDS*) e *honeypots* no âmbito tecnológico da empresa, mas sim examinar, interpretar e concluir sobre as informações abstraídas do fluxo de dados que estas tecnologias são capazes de produzir.

Este artigo sintetiza uma classificação com a qual o gestor de segurança estará gabaritado a projetar e diagnosticar dados não usuais em sua rede de computadores, identificando e enumerando as atividades maléficas em seu ambiente computacional. Assim, ele estará munido de informações críticas na construção de políticas eficazes para a proteção de seu perímetro de rede. O artigo está separado em 5 seções. Na seção 2 têm-se os trabalhos relacionados com o tema abordado. Na seção 3 detalham-se o projeto CLATH, sua contribuição científica e como o mesmo agrega vantagens para uma organização. Na seção 4 apresentam-se as formas de análise dos dados extraídos do sistema final. Por fim, na seção 5 são expressos os fatores de segurança em redes de computadores que promovem o CLATH a uma solução eficiente quando implantado corretamente em um ambiente computacional.

2 TRABALHOS RELACIONADOS

Entre os trabalhos relacionados à classificação de tráfego hostil está o desenvolvimento de taxionomias que propõem a identificação destes atos maléficos, assim como a sugestão de parâmetros que balizam sua classificação sob diversos aspectos. Papadaki *et al* (2002) apresenta a avaliação de uma taxionomia que prioriza, além da classificação, a ativação de respostas a possíveis incidentes. Estes pesquisadores exibem um número de incidentes genericamente identificados (vírus, *worm*, *buffer overflow*, acesso não autorizado, entre outros) e divididos em categorias cercando as formas mais comuns de ataque e os contextos que ocorrem estas incidências. Além disto, é apresentada uma avaliação dos possíveis impactos das vulnerabilidades sob a segurança, o tempo disponível de resposta e os ataques secundários que podem ser iniciados após um ataque principal.

Apesar de abrangente e detalhada, esta taxionomia tem limitações, como a falha em especificar o destino do ataque sem quantificar o número de sistemas alvo atingidos. Isto poderia ser considerado para compor o resultado final do incidente e nível de dano resultante. Atenta-se ainda para a não percepção no modelo da inclusão de propriedades de segurança como, o não-repúdio e autenticidade na avaliação do efeito de um incidente.

Outro método é proposto por Hansman e Hunt (2005) e resume-se em prover uma taxionomia holística e pragmática para abordar problemas inerentes a sistemas computacionais e ambientes de rede. Neste projeto todas as etapas da ação de um ataque são consideradas sem perder a especificidade. Hansman e Hunt (2005) baseiam-se no que denominam de dimensões. As **dimensões** são detalhes ou características de um ataque como, "Ataques de Rede" (d1), "Ataques em Aplicação Web" (d2) e "Fraude em Cookies" (d3). Elas fornecem uma visão mais clara do problema, pois realiza-se uma abordagem de maneira quantitativa e qualitativa aos ataques existentes no âmbito computacional, utilizando-se dimensões abrangentes e detalhistas. O conceito de dimensões é derivado também para os alvos dos ataques, como "Software" (d1), "Sistema Operacional" (d2), "Família Unix" (d3), "FreeBSD" (d4) e "5.1" (d5). As dimensões mostraram aspectos novos, não encontrados em outros modelos, que permitem uma análise mais minuciosa sobre a ação do atacante. Como ponto negativo, percebe-se a não preocupação em agregar as propriedades de segurança com as ações das hostilidades.

Propondo uma abordagem detalhada no projeto de taxionomia de segurança da Internet, Abbas, El-Saddik e Miri (2006) basearam-se nos serviços de rede para classificar as hostilidades, além de mapear as contramedidas para evitar ou combater cada uma delas. Esta classificação proposta por Abbas, El-Saddik e Miri (2006) consiste em uma lista de categorias, que representam os atuais e potenciais ataques de segurança que podem objetivar um sistema computacional.

A pesquisa de Abbas, El-Saddik e Miri (2006) exibe um novo ponto de vista envolvendo a interação das propriedades de segurança com as hostilidades atuais. É válido ressaltar igualmente a descrição das categorias dos ataques de segurança, sendo contemporânea e conceitualmente dividida. Como desvantagem é notório descrever a não preocupação em mensurar o quanto cada tipo de hostilidade afetaria as propriedades de segurança. Além disso, a não abordagem dos níveis de riscos sobre cada classe de ataque é preocupante, pois não permite avaliar a profundidade dos perigos abertos por uma hostilidade.

Por fim, a compreensão das fraudes computacionais, quantificando-as corretamente e inibindo seu risco de acontecimento são os objetivos principais do trabalho de Vasiu e Vasiu (2004). Neste modelo de classificação as hostilidades são denominadas como fraudes computacionais e são explicadas abordando os elementos da fraude e o ato da fraude. Outro item observado no modelo em questão, é a distinção realizada do tipo de atacante, sendo separados em *insiders* e *outsiders*.

Vasiu e Vasiu (2004) comprovam que grande parte das fraudes acontece dentro do perímetro de segurança do ambiente computacional, ação esta de propriedade do atacante intitulado com *insider*, que encontra facilidades, pois compreende o sistema computacional, suas fraquezas e seus pontos de entrada. Mas credita também outra parcela dos ataques por parte dos *outsiders*, que precisam somente representar um usuário válido ao sistema computacional para burlar o sistema, explorando uma vulnerabilidade ou oportunidade falha.

Diante disso propõe-se uma taxionomia, com uma perspectiva de prevenção, respeitando a plataforma e o método de perpetração – também se utilizando níveis ou dimensões. Como pontos fracos nesta abordagem, destacam-se a não apresentação de algumas pragas virtuais já

identificadas em modelos precedentes, além de categorias que poderiam ser mais exploradas por meio das propriedades de segurança.

Os modelos gerais de classificação de hostilidades serviram na fundamentação do CLATH. As carências encontradas nas classificações estudadas foram abordadas e elencadas, procurando saná-las nesta nova proposta de classificar hostilidades.

3 SISTEMA CLATH

Fundamentado por modelos precedentes e apoiando-se em suas vantagens e desvantagens, o sistema CLATH vem dispor uma nova saída para buscar a maturidade ideal de controle sobre as hostilidades de um ambiente de rede. O objetivo do CLATH é projetar uma classificação para o tráfego hostil em uma rede de computadores, a fim de auxiliar organizações a conhecer as maleficidades de seu âmbito computacional. Este projeto trata uma hostilidade procurando especificar valores de acordo com o negócio da organização a ser avaliada. Para mostrar a essência do CLATH, apresenta-se na Figura 1 a síntese de seu funcionamento.

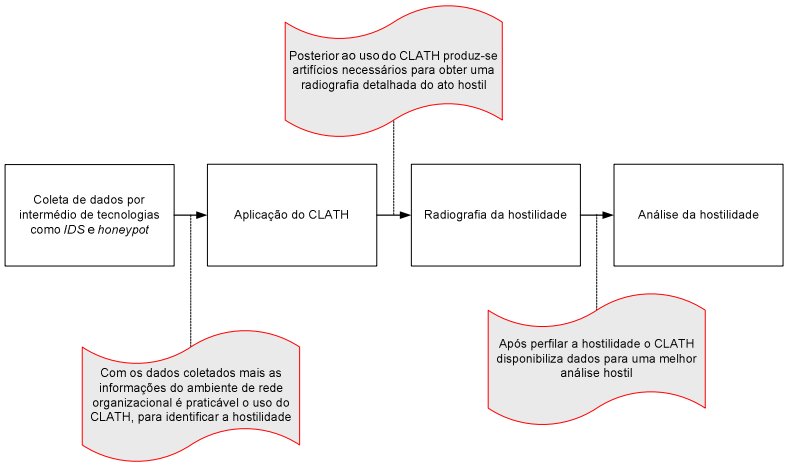

Figura 1: Ações na Identificação de Hostilidades pelo CLATH.
Fonte: Dos Autores (2008)

Na Figura 1 nota-se que a ação inicial exigida para analisar a segurança de um ambiente computacional aborda o levantamento de dados do tráfego deste e ainda, as informações pertinentes da rede de computadores a ser estudada, como sua abrangência e serviços providos. Para isso é necessária a coleta de dados por meio de tecnologias de segurança (*IDS* e *honeypot)*, além de profissional apto para detalhar os dados da organização.

Após a coleta destes dados, faz-se necessário aplicar o CLATH e iniciar a abstração de quão perigoso é a hostilidade encontrada. Posterior a aplicação do CLATH tem-se o perfil da hostilidade que foi dirigida ao sistema computacional alvo. Com este esboço maléfico é possível analisar de maneira mais detalhada o problema relacionado à segurança computacional. É importante notar que o ciclo exibido na Figura 1 funciona na busca sobre as informações de uma única hostilidade, sendo necessário ao dispor de um amplo número de dados maléficos, realizar este mesmo processo em cada hostilidade.

O sistema CLATH foi criado para atuar de modo segmentado e dependente, ou seja, possui dois núcleos de funcionamento, onde inicialmente coletam-se informações sobre o ato hostil e seqüencialmente conclui-se o nível de perigo da hostilidade encontrada. Primeiro é visto a ação do atacante, desde a entrada da hostilidade em um ambiente antes avaliado como seguro, até os efeitos causados por esta ação, sendo feita uma coleta de informações para identificar e pontuar que danos o atacante pode trazer ao ambiente computacional. Após são reunidas as informações requeridas para dar-se a pontuação final da hostilidade e totalizar o quanto uma

rede é considerada hostil. Atenta-se que o CLATH não atua como tecnologia para detecção de ataques e sim opera com dados hostis que estas tecnologias capturam.

3.1 FLUXOGRAMA DE IDENTIFICAÇÃO HOSTIL

O fluxograma da Figura 2 é o núcleo de funcionamento do CLATH. Ele depende ativamente de três processos atrelados e cada um deles possui um fluxograma independente, de identificação hostil, sendo identificado por uma numeração seqüencial.

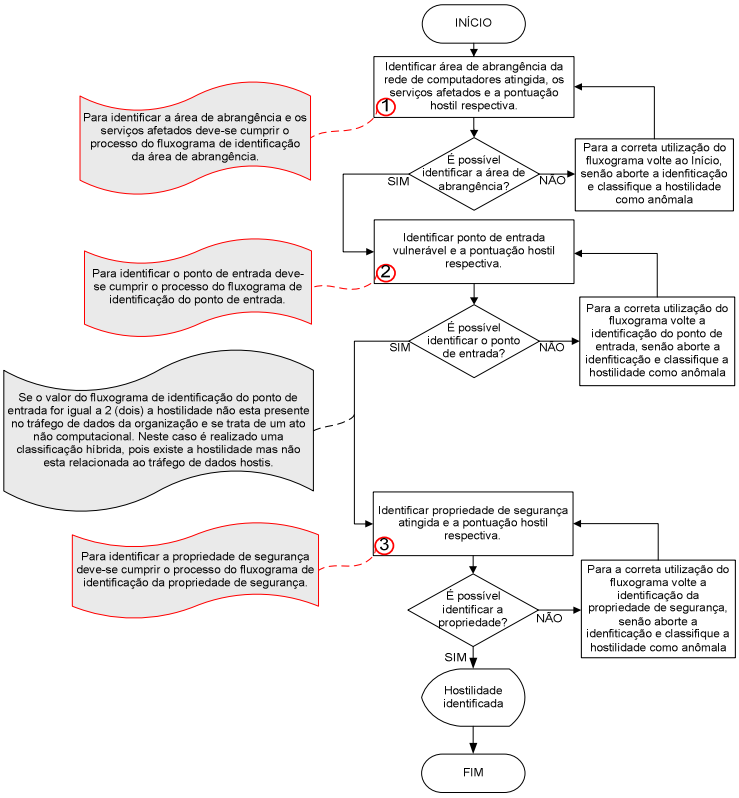

Figura 2 : Fluxograma de Identificação Hostil
Fonte: Dos Autores (2008)

Nota-se na Figura 2 que os três processos pertencentes ao fluxograma de identificação hostil estão numerados de 1 a 3. Esta é a ordem a ser seguida para uma hostilidade ser corretamente avaliada pelo CLATH. É importante observar, além disso, que as hostilidades são identificadas individualmente e para saber o verdadeiro comprometimento de seu negócio deve ser aplicado o funcionamento por completo do CLATH: classificação e análise de dados.

3.1.1 Área de abrangência da hostilidade

Ao tratar a área de abrangência, questiona-se o grau de extensão do dano de uma possível hostilidade. O relevante deste aspecto é determinar o quão prejudicial uma ação hostil pode vir a ser dependendo da rede afetada.

Em uma *WAN*, por exemplo, o atacante ao utilizar a técnica de espionagem contra um sistema computacional pode afetar múltiplos serviços de acesso público e com isso o grau de avaria é maior devido à abrangência de uma rede *WAN*. Mas, se o ataque for disparado a uma rede de menor abrangência, por exemplo, a uma rede *LAN* então este pode ter um impacto menos significante. Todavia para não classificar o nível de hostilidade de uma rede de computadores erroneamente, outros dois aspectos devem ser considerados. O primeiro é a quantidade de redes (independente do tipo de abrangência) condicionadas a rede alvo do ataque. Assim

quando uma *WAN* for atacada, além da pontuação auferida por o ataque ser efetuado neste tipo de rede, o número de redes diretamente interconectadas também serão avaliadas. Aliado a isto, se tem como outro parâmetro qualificador, o número de serviços públicos oferecidos dependentes do alvo avariado - rede atingida e diretamente conectada.

Para pontuar um ataque quanto a sua área de abrangência foi adaptado e produzido um paralelo aos conceitos de Branigan (2002). Nestes conceitos descreve-se que o grau do risco quanto ao seu impacto para o negócio da organização pode ser classificado em: alto, médio e baixo. Na classificação da área de abrangência foram aproveitados os níveis de risco de Branigan (2002) com inserção de dois índices medianos, como é visto na Tabela 1.

Tabela 1 - Pontuação da Área de Abrangência

Gravidade	**Pontos**	**Descrição**
gravíssimo	5	Redes de grande abrangência e com possibilidades de ao não ser combatido o problema, este piore imediatamente.
muito grave	4	Para redes de abrangência grande a média no qual o problema não sendo sanado, deve piorar a curto prazo.
gravidade moderada	3	Relaciona-se a redes com alcance médio, no qual a hostilidade não sendo inibida, acarreta uma piora a médio prazo do problema a ela atrelado.
pouco grave	2	Para redes de abrangência média a pequena com piora a longo prazo do problema contraído por não ser combatido.
sem gravidade	1	Indica redes de pequena abrangência e comprometimento baixo de serviços providos, no qual a hostilidade não tem tendência de piorar.

Fonte: Dos Autores (2008)

Além da pontuação pela identificação do tipo de abrangência da rede alvo, como exibido na Tabela 1, se atribui à pontuação mínima (1 ponto) para cada serviço indisponível provido pela rede de computadores afetada ou redes diretamente conectadas. Para esta pontuação ser efetuada, assim que cada serviço for comprometido (por exemplo: *HTTP*, *DNS*, *SSH* e *FTP*) é acrescido "1" ponto na contagem hostil da rede envolvida ou diretamente conectada. Esta pontuação hostil quanto a serviços deve ser concedida para a rede afetada e as diretamente conectadas. O funcionamento da identificação da área hostilizada é realizado pelo fluxograma disposto na Figura 3 - parte 1 do processo de identificação hostil.

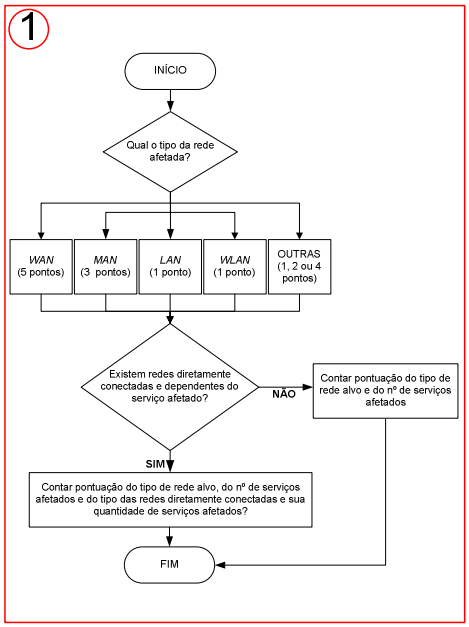

Figura 3 : Fluxograma para Identificação da Área de Abrangência Afetada
Fonte: Dos Autores (2008)

No fluxograma da Figura 3 nota-se como primeiro passo à escolha do tipo de rede afetada. Após a definição do tipo de rede atribui-se a pontuação relacionada à área de abrangência. Uma nota importante, neste caso, é designada às redes que intituladas como "outras" diferem das redes *WANs*, *MANs*, *LANs* e *WLANs*. Exemplos são a *Storage Área Network (SAN*), a *Personal Área Network (PAN*) e a *Campus Area Network (CAN*).

Após a definição do tipo de rede que sofreu o dano diretamente, questiona-se sobre a existência de redes diretamente conectadas e serviços afetados com a hostilidade. Caso a resposta à indagação seja negativa, pontua-se a rede afetada mais o número de serviços afetados e finaliza-se o fluxograma para identificação da área afetada. Mas respondendo positivamente pontua-se a rede diretamente afetada mais o número de serviços diretamente afetados adicionando a pontuação das redes afetadas diretamente conectadas e serviços atingidos encerrando-se assim o processo de identificação da área de abrangência.

Qualificando desta forma uma rede de computadores inova-se as classificações existentes de tráfego hostil, que em grande parte quantificam somente o ataque e não a abrangência e destruição causada por ele. De posse desta pontuação a organização alvo é analisada de acordo com a real abrangência do dano causado pela hostilidade, visto que além de detectar o tipo rede afetada permite-se a moldagem dos ambientes e serviços atingidos.

3.1.2 Ponto de entrada da hostilidade

O segundo item do fluxograma de identificação hostil relaciona qual tipo de situação é conivente para a ação do atacante. Aqui se identifica que ponto vulnerável do ambiente computacional permite que uma hostilidade adentre em contato com o alvo a ser atingido e, análogo à área de abrangência, a pontuação dos elementos deste fluxograma, é baseada em literaturas como Branigan (2002). Deve-se, no entanto, conhecer os elementos do fluxograma que define o ponto de entrada pelo qual o atacante infringiu a segurança computacional.

Caracterizar o sistema computacional origem que permitiu a entrada da hostilidade é o primeiro elemento necessário para o entendimento do fluxograma de identificação do ponto de entrada vulnerável. Ao tratar dos sistemas computacionais, quatro tipos são considerados neste projeto de classificação de tráfego. Partindo de definições originárias de Papadaki *et al* (2002), os sistemas computacionais passíveis de identificação são os definidos na Tabela 2.

Tabela 2 - Sistemas Computacionais Alvos dos Ataques

Sistema Computacional	**Descrição**
servidores externos (5 pontos)	Dispostos publicamente provendo serviços como: *HTTP*, *FTP*, *DNS* e *E-MAIL*.
componentes de rede (3 pontos)	Utilizados na comunicação dos ambientes de rede, como os roteadores e *switches*, podendo ser dispostos publicamente ou não.
servidores internos (3 pontos)	Presentes na *intranet* da organização. Exemplos são o servidor de arquivos e controlador de domínio.
estações de trabalho (1 ponto)	Aplicados a realizar operações específicas de assuntos afins a sistemática da organização.

Fonte: Dos Autores (2008)

Os servidores externos tiveram sua pontuação considerada máxima (5 pontos) por causa de sua importância elevada devido à exposição pública e habitual dificuldades de substituição caso sofram alguma avaria. Já os componentes de rede são aqui pontuados com 3 pontos, pois a interrupção dos mesmos pode gerar incômodos críticos como paralisação completa de uma organização. Quanto aos servidores internos em uma organização, são pontuados com 3 pontos quando comprometidos, seguindo a mesma premissa dos servidores externos.

Entretanto, com atenuação de serem servidores internos a organização, tem dessa forma a abrangência do problema isolada. Por fim, com pontuação mínima quanto a problemas com hostilidades encontram-se as estações de trabalho.

Após a identificação do tipo de sistema computacional no qual resultou a ação com sucesso do atacante é necessário entender a situação que permitiu este ato hostil. Neste projeto de classificação de tráfego hostil os pontos de entradas falhos de um ambiente computacional são divididos segundo a Tabela 3.

O primeiro ponto de entrada a ser abordado são casos relacionados a vulnerabilidades de cunho não computacional - as vulnerabilidades humanas, naturais e físicas. Todos estes problemas são designados como um ponto de entrada chamado de ato não computacional. Não serão subdivididas estas hostilidades não computacionais para fins de pontuação no fluxograma, sendo as mesmas tratadas em um só conceito. Uma nota importante a destacar-se é que o ato não computacional é um tipo de entrada vulnerável que pode ou não gerar tráfego hostil. Se ocorrer, por exemplo, um incêndio em uma organização ocorrerá uma indisponibilidade de seus sistemas computacionais, no entanto, isto não foi gerado por tráfego hostil. Mesmo assim, decorrente do previsto pelo fluxograma de identificação do ponto de entrada esta situação resultar-se-ia em 2 pontos hostis.

Tabela 3 - Detalhamento dos Pontos de Entrada

Ponto de Entrada	**Pontos**	**Descrição**
ato não Computacional	2	Vulnerabilidades físicas, humanas e naturais são associadas a este ponto de entrada.
dispositivo de hardware	2	São pontuados aqui itens relacionados à falhas de hardwares em sistemas computacionais.
recurso de rede	4	Abrange recursos de rede, ou seja, os serviços, portas ou protocolos indevidamente utilizados.
recurso de software	condicional	São pontuados falhas de SO ou aplicativos.

Fonte: Dos Autores (2008)

Explicando os atos não computacionais têm-se as vulnerabilidades relacionadas a recursos humanos que condizem com ações de colaboradores da organização e seus atos não propícios para a segurança organizacional. Questões como falta de treinamento e comprometimento com as práticas de segurança, bem como, o uso inadequado de tecnologias e compartilhamento indevido de dados são problemas que podem levar a uma ação hostil.

Outra vulnerabilidade não computacional também tratada são questões físicas que envolvem as organizações. Estas são relacionadas às propriedades físicas encontradas no ambiente organizacional que podem afetar recursos tecnológicos como ambientes tecnológicos mal projetados, instalações elétricas incorretas e acesso físico impróprio de terceiros ao ambiente tecnológico crítico da organização.

Os atos de atacantes referentes a vulnerabilidades encontradas em hardwares é o segundo ponto de entrada abordado. O conjunto de hardware aqui abrange obsolescência, tempo de vida útil, desgaste, ou falha não prevista de um dispositivo. Uma organização, ao adotar o CLATH, se vir a ser invadida por uma vulnerabilidade em hardware esta deve adicionar 2 pontos ao fluxograma da identificação do ponto de entrada. Isto se justifica por dispositivos de hardwares problemáticos, na maioria das vezes, constituírem problemas pontuais sendo solucionados pela substituição do item ou atualização de *firmware*.

Os recursos de rede são a terceira possibilidade de ponto de entrada vulnerável permitido pelo CLATH. Capacita-se neste ponto de entrada identificar três tipos de elementos vulneráveis relacionados a recurso de rede: porta, protocolo e serviço, expostos na Tabela 4.

Tabela 4 - Recursos de Rede Identificados pelo CLATH

Recurso de Rede	**Pontos**	**Descrição**
Porta	4	Hostilidades que objetivam explorar determinada porta.
Protocolo	4	Aqui são encontradas falhas presentes em protocolos de rede como o *TCP*, *IP*, *ICMP* e *UDP*.
Serviço	4	O atacante busca determinado serviço independente sob qual porta este se encontra alocado.

Fonte: Dos Autores (2008)

Referente à Tabela 4 o item porta traz a abrangência de ataques no qual se procura infringir um sistema computacional com ação hostil encaminhada a uma determinada porta que provê um determinado tipo de serviço. Estas hostilidades que objetivam referenciar a porta de um sistema computacional, geralmente atacam as portas padrões dos serviços providos por sistemas operacionais. O ataque neste caso não se preocupa em conhecer realmente a existência de algum serviço sendo executado na porta a ser atacada, ou se a porta está habilitada com o serviço padrão. O escopo do ataque então é gerar danos encaminhando tráfego hostil para determinada porta imaginando que o serviço padrão está nesta configurada.

Outro item referente a um ponto vulnerável de entrada num recurso de rede é o protocolo sob qual o tráfego desta rede funciona. A interligação em redes de comunicação abriga a existência de vários padrões de protocolos de comunicação. Estes protocolos, como o *TCP*, *IP*, *UDP*, *AppleTalk*, *IPX* entre outros, possuem fragilidades, como falhas relacionadas à autenticidade, privacidade ou integridade dos dados, não permitindo então segurança completa na troca de dados entre os sistemas computacionais. Se enquadram aqui, os ataques que se aproveitam das fragilidades dos protocolos de comunicação de rede e burlam sistemas computacionais. O terceiro item listado na Tabela 4 trata dos ataques dirigidos a serviços providos por sistemas computacionais públicos. Diferente dos ataques a portas configuráveis nos sistemas operacionais, estes ataques buscam falhas nos serviços como o *FTP* e *SSH* para realizarem investidas hostis. Eles independem de portas e objetivam sempre falhas nestes serviços como o uso incorreto ou impróprio de configurações.

Todos estes ataques referentes a pontos de entrada vulneráveis em recursos de rede recebem no CLATH 4 pontos hostis para a documentação do processo de análise de identificação. Esta pontuação justifica-se por todos estes recursos, porta, protocolo e serviço, dispostos no sistema computacional, permitirem ataques comuns ao mesmo como documentado em Pfleeger e Pfleeger (2003) e Gangemi, Lehtinen e Russell (2006).

O quarto ponto de entrada classificado pelo CLATH está relacionado a vulnerabilidades dirigidas a softwares. Esta classificação (Tabela 5) sofre uma divisão baseada em Langweg e Snekkenes (2004), onde se define que um atacante pode dirigir hostilidades a sistemas operacionais e aplicativos.

Tabela 5 - Recursos de Software Identificados no CLATH

Recurso de Software	**Pontos**	**Descrição**
sistema operacional	5	Vulnerabilidades relacionadas a tentativas de ataques específicas em burlar falhas de sistemas operacionais.
Aplicativo	4	Condizem com problemas de aplicativos que são explorados por atacantes.

Fonte: Dos Autores (2008)

Os ataques relacionados a sistemas operacionais recebem pontuação 5 no fluxograma de identificação do ponto de entrada vulnerável. Isto é justificado devido à criticidade existente em toda interoperabilidade realizada entre o hardware e o usuário ser de responsabilidade do SO, tendo este papel fundamental em todas as ações do sistema computacional.

Já os ataques que exploram aplicativos dos mais diversos fins para tentarem fraudar o sistema computacional são explicados pelo CLATH baseados no modelo de Langweg e Snekkenes (2004), que retratam grande importância para os problemas existentes em aplicativos. Este tipo de ataque adiciona 4 pontos ao fluxograma de identificação do ponto de entrada vulnerável de um sistema computacional. Sua pontuação não foi elevada ao máximo quanto às investidas hostis realizadas contra SOs, devido ao seu comprometimento normalmente ser relacionado a situações mais restritas dentro do âmbito geral de um sistema computacional. Complementado a descrição de todos os elementos possíveis no uso do fluxograma de identificação do ponto de entrada hostil é necessário exibir, como segue na Figura 4, o funcionamento do fluxograma para melhor entendimento.

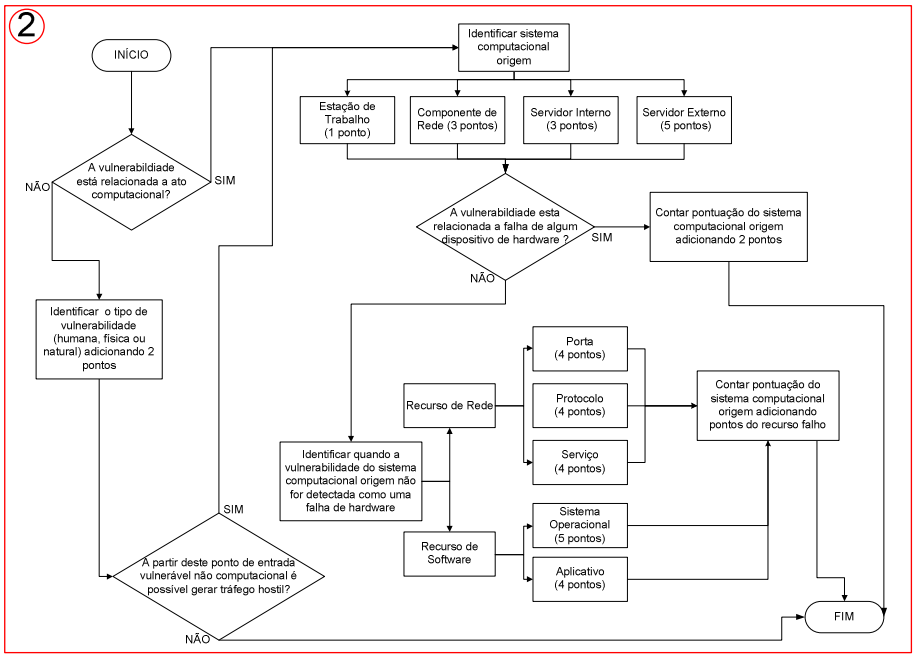

Figura 4: Fluxograma de Identificação do Ponto de Entrada
Fonte: Do Autor (2008)

Após a análise da área de abrangência por meio do fluxograma de identificação específico é necessário seguir para o próximo passo para conhecer qual hostilidade está sendo direcionada a organização alvo. No fluxograma de identificação do ponto de entrada exibido na Figura 4 inicia-se o processo de análise verificando se a hostilidade encontrada é relacionada a algum ato não computacional. No caso da ação hostil não ser atrelada a algum ato computacional, é necessário identificar se a partir da mesma é possível gerar tráfego hostil, como na ocorrência de um ato de engenharia social para adentrar na organização.

Ao identificar o sistema computacional originário da hostilidade a organização afetada pode optar por três opções, devidamente pontuadas para a finalização da pontuação hostil. Seguindo o fluxograma, o próximo passo permite associar a hostilidade referida segundo algum problema de hardware nos sistemas computacionais, antes identificados, que permitiu a entrada da hostilidade. Se o problema for realmente relacionado a algum item de hardware o processo de identificação hostil é finalizado somando-se os pontos hostis durante o fluxo percorrido. Contudo, ao não se tratar de um problema relacionado a hardware permite-se

ainda determinar se a hostilidade está associada a um recurso de software ou de rede, que possibilitam derivações específicas em cada caso.

Com o detalhamento dos pontos de entrada considerados pelo CLATH capacita-se a organização, até este momento, a somar três elementos na análise para identificar hostilidades: **a área de abrangência** e **os serviços afetados pela hostilidade** e que **ponto de entrada** foi utilizado para permitir esta invasão. A partir de agora, na seção 3.1.3 é visto a relação dos ataques com as propriedades de segurança.

3.1.3 Propriedade(s) de segurança afetada(s) pela hostilidade

Com a classe de ataque já definida é necessário, para finalizar a identificação hostil, descobrir qual propriedade de segurança é afetada. Diante de vastas classificações foi necessário limitar as técnicas de ataques, assim exposto na Tabela 6, perante as classes de ataques conceituadas por Stallings (2006) para o fluxograma de identificação da propriedade afetada resultar em uma correta pontuação hostil.

Tabela 6 - Técnicas de Ataque Relacionadas à Classe de Ataque

Classe	**Técnica de Ataque**
interceptação	análise de trafego
	divulgação do conteúdo de mensagens
	Snooping
	Probe / scan, sniff (active sniffing)
Interrupção	*denial of service*
	distributed denial of service
	destruição de hardware
modificação	forjamento de mensagens
	registro da base de dados alterado
Fabricação	*Masquerade*
	Replay
	ip spoofing
	Baseado em senha
	Baseado na exploração do acesso confiável

Fonte: Dos Autores (2008)

Depois da definição da técnica de ataque e o entendimento a qual classe esta pertence, deve-se concluir o fluxograma de identificação da propriedade afetada que é demonstrada na Figura 5, para conhecer a qual propriedade de segurança a hostilidade se dirigiu. A definição de qual propriedade de segurança foi atingida segue as definições de Stallings (2006) que respectivamente atrela as classes de ataque interceptação, interrupção, modificação e fabricação das propriedades de segurança confidencialidade: disponibilidade, integridade e autenticidade/nãorepúdio. O fluxograma apresentado na Figura 5 inicia-se o processo já com a classe da técnica de ataque definida. Esta definição ocorreu no resultado obtido do fluxograma de identificação do ponto de entrada juntamente com a análise da Tabela 6.

Conhecida a classe de ataque é necessário indicar qual propriedade esta classe compromete pontuando-a e finalizando assim o processo de identificação da hostilidade. A pontuação hostil determinada para as propriedades de segurança baseia-se em autores como Landwehr (2001), Pfleeger e Pfleeger (2003) e Gangemi, Lehtinen e Russell (2006) que definem como

fundamentais as propriedades disponibilidade, confidencialidade e integridade, tendo assim, esta pontuação maior por parte do fluxograma caso venham a ser afetadas.

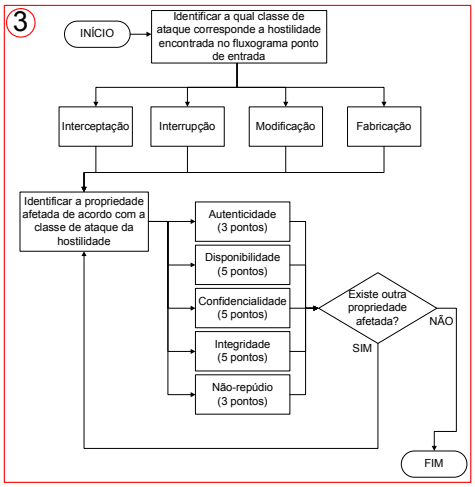

Figura 5: Fluxograma de Identificação da Propriedade Afetada
Fonte: Dos Autores (2008)

Vale ressaltar na Figura 5, que ao ter-se mais de uma propriedade de segurança afetada o processo repete-se e a pontuação é cumulativa. Assim sendo deve-se executar novamente o fluxograma de identificação da propriedade afetada somando-se os valores correspondentes das propriedades atingidas. Em seguida a identificação da propriedade afetada pela ação da hostilidade o processo de execução do fluxograma de identificação hostil é finalizado, e passa-se a ter as características essenciais para personificar a organização atingida. No entanto, para complementar o CLATH é necessário analisar os dados decorridos da execução do fluxograma de identificação hostil.

4 ANÁLISE DE DADOS DO CLATH

Ao analisar os dados resultantes obtidos por meio do fluxograma de identificação hostil, acionam-se três eventos - obrigatoriamente seqüenciais - que completam a ação dos fluxogramas na identificação de uma hostilidade. O primeiro evento é a tabulação da avaliação do resultado dos fluxogramas, de maneira que facilite a compreensão da hostilidade. O segundo evento determina o quanto os valores hostis, obtidos no primeiro evento, representam perigo à organização. E por fim, o terceiro evento representa o valor numérico hostil que identifica o grau de comprometimento da hostilidade analisada para a organização.

4.1 MATRIZ DE DECISÃO

Denomina-se matriz decisão o primeiro evento na análise de dados hostis pelo sistema CLATH. Representando o funcionamento da matriz decisão, a Tabela 7 mostra todos os elementos do fluxograma passíveis de análise pela organização.

A matriz decisão prevê que a cada hostilidade investigada por parte do fluxograma de identificação hostil, esta seja acompanhada pela inserção de seus dados hostis (propriedades da hostilidade), resultantes da ação dos fluxogramas, em seus respectivos campos propícios para o recebimento destes valores. A utilização da matriz decisão, como também mencionado aos fluxogramas, deve acontecer individualmente para cada hostilidade.

Para explicar o funcionamento de uma matriz decisão, exibido na Tabela 7, analisa-se um ataque *DOS* (*denial of service*). O cenário deste ataque é uma rede *MAN* (rede metropolitana)

que possui outras 15 (quinze) redes *LANs* dependentes. A rede *MAN* atacada teve seu serviço de *gateway* comprometido por um ataque *DOS*. Deste *gateway*, disposto em forma de hardware é provido a conexão do acesso para exatamente 15 (quinze) redes *LANs* usufruírem do serviço *HTTP*. A propriedade afetada em um ataque *DOS* é a disponibilidade. Com todos os dados do cenário deste ataque fica facilitada, após o processo de análise por meio do fluxograma, a inserção de dados sobre a matriz decisão.

Tabela 7 - Exemplo de Utilização da Matriz Decisão

PERFIL DA HOSTILIDADE		**Ataque = *DOS***	
Itens de avaliação	**Peso**	Quantidade	Pontuação final
Área de Abrangência (AA)			
wan	5	NA	NA
man	3	1	3
lan	1	15	15
wlan	1	NA	NA
outra			
tipo 1	1	NA	NA
tipo 2	2	NA	NA
tipo 3	4	NA	NA
resultado de (AA)			**18**
Serviços Afetados (SA)	1	2	2
resultado de (SA)			**2**
Ponto de Entrada (PE)			
servidor externo	5	NA	NA
servidor interno	3	NA	NA
componente de rede	3	1	3
estação de trabalho	1	NA	NA
software			
sistema operacional	5	NA	NA
aplicativo	4	NA	NA
hardware	2	1	2
ato não computacional	2	NA	NA
rede de computadores	4	NA	NA
resultado de (PE)			**5**
Propriedade Afetada (PA)			
confidencialidade	5	NA	NA
Integridade	5	NA	NA
disponibilidade	5	1	5
não-repúdio	3	NA	NA
autenticidade	3	NA	NA
resultado de (PA)			**5**

Fonte: Dos Autores (2008)

Além do exemplo do ataque *DOS*, exibido na Tabela 7, é propício entender cada um dos campos da tabela matriz decisão. Na primeira coluna estão todos os elementos presentes nos fluxogramas e necessários para a pontuação da hostilidade. A segunda coluna tem o peso de cada elemento já fundamentado nas seções anteriores. A terceira coluna chama-se quantidade e referencia o número de elementos envolvidos durante o processo hostil indicado pelo fluxograma. Então, por exemplo, se em uma ação hostil seis redes *LANs* forem atingidas a célula correspondente à rede *LAN* relacionada à coluna quantidade recebe a pontuação 6. Por

fim a coluna pontuação final recebe o resultado do peso de cada elemento participante do processo hostil multiplicado a quantidade de vezes que este apareceu no ato maléfico.

4.2 CÁLCULO DO ÍNDICE HOSTIL

Depois do preenchimento da matriz decisão é necessário utilizar os valores resultantes dos índices hostis, a fim de avaliá-los e entender a gravidade da hostilidade. Para compreender os valores dos índices hostis é necessário realizar o cálculo do índice hostil. Neste cálculo há quatro valores que foram identificados com auxílio dos três fluxogramas específicos e tabulados pela matriz decisão que serão utilizados.

Estes valores são os índices hostis área de abrangência (AA) e serviços afetados (SA) que foram abstraídos no primeiro fluxograma, chamado fluxograma de identificação da área afetada. O índice ponto de entrada (PE), que foi resultante do fluxograma de identificação do ponto de entrada vulnerável e por fim, o índice propriedade afetada (PA), que resultou do processo do fluxograma de identificação da propriedade afetada.

Com os valores destes índices hostis computados e definidos é necessário usá-los no cálculo do índice hostil. Para isto, cada índice hostil depois da atribuição do valor numérico deve ser medido em muito grave, grave ou pouco grave. A importância destes intervalos, representados na Tabela 8, foi designada conforme explicações prévias junto à concepção dos fluxogramas e são fundamentados em práticas empíricas e por índices usados ao decorrer da análise dos outros modelos taxonômicos.

Tabela 8 - Cálculo do Índice Hostil

	muito grave = 5 pontos	**grave** = 3 pontos	**pouco grave** = 1 ponto
área de abrangência (AA)	$(AA) \geq 5$	$2 \leq (AA) < 5$	$(AA) < 2$
serviço afetado (AS)	$(SA) > 3$	$(SA) = 3$	$(SA) < 3$
ponto de entrada (PE)	$(PE) \geq 7$	$7 > (PE) > 3$	$(PE) \leq 3$
propriedade afetada (PA)	$(PA) > 6$	$6 \geq (PA) > 3$	$(PA) = 3$

Fonte: Dos Autores (2008)

Na Tabela 8 são expostos os índices hostis e os possíveis intervalos que os valores numéricos resultantes da ação dos fluxogramas podem assumir. Estes valores podem variar como já citados, em três níveis. Sendo avaliados estes índices podem ser tratados em muito grave, grave e pouco grave recebendo pontuação respectiva de 5 (cinco), 3 (três) e 1 (um) ponto. Então a partir da ação de uma hostilidade, cada índice hostil resultante da matriz decisão pode variar de 1 a 5 pontos sua gravidade final.

Por conseqüente, sendo utilizados quatro índices para avaliar a pontuação final de uma hostilidade, à somatória dos valores destes índices, a partir da Tabela 8, é que irá determinar que grau de hostilidade um determinado ataque conseguiu atingir. Sendo assim uma hostilidade pode alcançar diferentes níveis de gravidade entre os índices hostis, mas somente a soma dos níveis de gravidade destes quatros índices é que irão determinar o número final hostil que representará o grau de preocupação referente à hostilidade detectada.

Mostra-se à prática da utilização no cálculo do índice hostil, empregando o exemplo já referido ao demonstrar a utilização da matriz decisão na Tabela 7, um ataque *DOS*. Neste caso

então como índices resultantes na Tabela 7 tem-se os valores de (AA)=18, (SA)=2, (PE)=5 e (PA)=5. Nota-se que dos índices calculados um destes, o (AA) é tido como muito grave, pois o mesmo é maior que cinco; dois deles, (PE) e (PA), foram tidos como graves e o único índice gabaritado com pouca gravidade foi o (SA). É necessário entender que estes valores dos índices hostis indicados por meio da matriz decisão são usados para obter o nível de gravidade de cada índice. Na Figura 6, tem-se uma demonstração do cálculo do índice hostil, utilizando o exemplo do ataque *DOS*, já mencionado na matriz decisão.

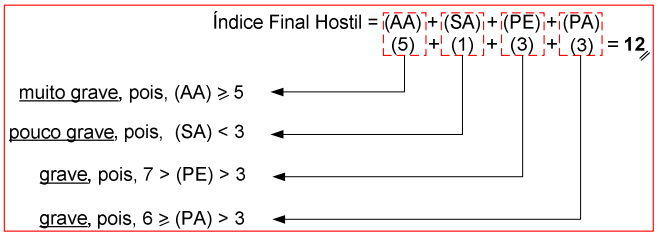

Figura 6: Demonstração de Uso no Cálculo do Índice Hostil
Fonte: Dos Autores (2008)

Os dados da Figura 6 exibidos perfaz-se um valor final de 12 pontos hostis decorrentes do ataque *DOS*, antes explicado. Observa-se que os índices hostis podem variar incondicionalmente o que torna a abrangência de solução por meio do CLATH mais coerente, visto a variância do tipo de hostilidades e estruturas organizacionais. Após a definição da pontuação final da hostilidade é necessário verificar, por fim, que conseqüências de impactos à segurança computacional a mesma ocasionará – foco da seção 4.3.

4.3 ÍNDICE FINAL DA HOSTILIDADE

Como terceiro e último processo da análise dos dados hostis capturados pelo fluxograma de identificação hostil é necessário avaliar o resultado final obtido com o cálculo do índice hostil. Este resultado final constitui-se da somatória de todos os índices hostis e esta totalização então representará o valor da hostilidade perante a organização afetada. Por exemplo, o 12 da Figura 6 é bom ou ruim para a organização?

Este resultado numérico, possibilita a hostilidade pontuar de 20 a 4 pontos hostis possíveis, devidos aos critérios estabelecidos no cálculo do índice hostil, Tabela 8. No entanto necessita-se entender este índice final da hostilidade. Para isto, foram divididas as possibilidades numéricas de acontecimento para o índice final hostil perfazendo três "conceitos" conforme a Figura 7, que diferencia o nível de cada pontuação.

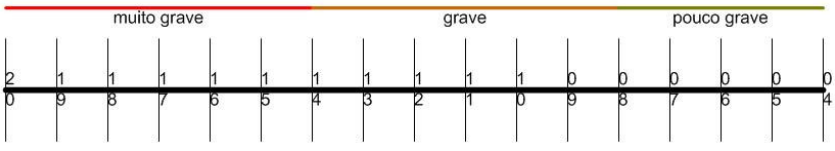

Figura 7: Índice Final Hostil
Fonte: Dos Autores (2008)

Este índice final hostil permite a hostilidade ser classificada como muito grave, (15 a 20 pontos), grave (9 a 14 pontos) ou pouco grave (4 a 8 pontos). Ao ser classificada como muito grave a organização deve-se preocupar ao máximo, pois dois ou mais índices entre (AA), (SA), (PE) e (PA) foram tidos como muito grave no cálculo do índice hostil, sendo isto um fato certo para interromper o negócio da organização.

Com o índice final hostil, o processo de identificação da hostilidade chega ao fim e a organização pode entender o quão está afetada por este problema encontrado em seu ambiente

computacional. Contudo, ao ter um grande número de hostilidades avaliadas é possível entendê-las criando um gráfico sobre a totalidade de atos hostis produzidos. Um exemplo é visualizado no Gráfico 1, que demonstra a análise de vinte hostilidades por meio do CLATH.

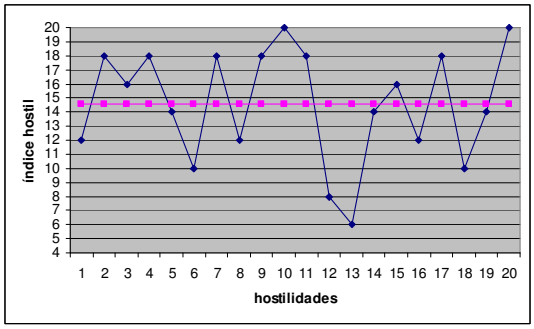

Gráfico 1 - Exemplo Fictício da Ação de Vinte Hostilidades
Fonte: Dos Autores (2008)

Como processo suplementar ao Gráfico 1 e para melhor caracterizar uma organização, o CLATH também pode ser aplicado a fim de gerar uma "nota" final a segurança de qualquer ambiente tecnológico. Esta "nota" avaliará em um intervalo de tempo estabelecido de coleta de dados à segurança de uma organização nos quais determinadas hostilidades foram avaliadas. Exemplificando este número final de segurança, seguindo a hipótese do Gráfico 1, apresentam-se vinte hostilidades cada qual já com o seu valor hostil agregado. Este número final, neste caso, é representado pela soma de todos os valores dispostos no Gráfico 1 que resultaria no valor final de 292 pontos hostis. Este número pode ser chamado de "**valor final da segurança de um ambiente tecnológico",** que neste exemplo avaliou uma organização fictícia por meio do CLATH com dados sobre vinte hostilidades coletadas.

A individualização da hostilidade e personificação da organização são vantagens causadas pelo CLATH. Diferente de outros modelos vistos, este projeto de classificação de tráfego hostil acata o negócio da organização para avaliar de maneira correta o efetivo emprego nocivo da hostilidade. O CLATH referencia todos os passos da ação de um ato hostil, desde a sua entrada na rede até o tipo de comprometimento ocorrido nos sistemas computacionais. Com a utilização do CLATH uma organização pode analisar suas hostilidades particularmente e melhor direcionar ações inibidoras na rede de computadores. É indispensável no CLATH o conhecimento sobre redes de computadores e segurança computacional para corretamente aplicar suas técnicas e processos.

5 CONCLUSÃO

Intrusões são constantemente diagnosticadas em rede de computadores, seja ela equipada ou não por tecnologias de segurança. Saber suportar o conteúdo maléfico de dados disparados a uma organização não passa apenas por configurar sistemas específicos de defesa, mas também entender suas aplicabilidades e informações que possam ser extraídas a partir destes. Estas informações abstraídas se bem compreendidas auxiliam na percepção do objetivo do ato hostil e conseqüências atreladas.

A individualização da hostilidade e personificação da organização são vantagens causadas pelo CLATH. Diferente de outros modelos vistos, este projeto de classificação de tráfego hostil acata o negócio da organização para avaliar de maneira correta o efetivo emprego nocivo da hostilidade. O CLATH referencia todos os passos da ação de um ato hostil, desde a sua entrada na rede até o tipo de comprometimento ocorrido nos sistemas computacionais. Com a utilização do CLATH uma organização pode analisar suas hostilidades particularmente e melhor direcionar ações inibidoras na rede de computadores. É indispensável no CLATH o

conhecimento sobre redes de computadores e segurança computacional para corretamente aplicar suas técnicas e processos.

O CLATH permite ao profissional especializado organizar as prioridades relacionadas à segurança, pois possibilita uma interoperabilidade maior entre as tecnologias que capturam intrusões e a análise dos registros por estas coletados. Benefícios como à melhora na qualidade e escrita de políticas de segurança, o entendimento do tráfego de dados presente no âmbito computacional, a compreensão de qual hostilidade representa maior perigo a rede de computadores, além de poder colaborar para a justificativa de investimentos em segurança do ambiente de rede, são sinônimos de vantagens encontradas na adoção desta proposta.

Como trabalho futuro sugere-se a aplicação do CLATH em algum cenário organizacional existente tendo com isto estabelecido a ideal interação entre todos os conceitos agregados no projeto proposto e as práticas hostis que venham a ser dirigidas a este exemplo de organização, servindo como prova de conceito. Completando as sugestões de trabalhos futuros percebe-se também a possibilidade de programação dos processos representados por meio dos fluxogramas, chegando assim ao sistema CLATH palpável, e a elaboração de métricas para comparação entre os diversos métodos de classificação de tráfego hostil.

REFERÊNCIAS

ABBAS, Ali; EL-SADDIK, Abdulmotaleb; MIRI, Ali. A comprehensive approach to designing internet security taxonomy. In: ELECTRICAL AND COMPUTER ENGINEERING CCECE '06. Canadian Conference on, 2006, Ottawa. **Proceedings...** Ottawa: IEEE, 2006. p. 1316-1319.

BARBATO, Luiz G. C.; MONTES, Antônio. Técnicas de monitoração de atividades em honeypots de alta interatividade. In: SIMPÓSIO SOBRE SEGURANÇA EM INFORMÁTICA, 5., 2003, São José dos Campos. **Anais...** São José dos Campos: INPE/LAC 2003. p. 100-108.

BRANDÃO, Antonio J. S.; MARTIMIANO, Luciana A. F.; MOREIRA, Edson S. O uso de ontologia em alertas de vulnerabilidades. In: SIMPÓSIO BRASILEIRO DE REDES DE COMPUTADORES, 22., 2004, Gramado. **Anais...** Gramado: USP, 2004. p. 75-86.

BRANIGAN, Steven. Securing the critical IP infrastructure. **Information Security Technical Report**, v. 7, n. 2, p. 57-64, June 2002.

CAMPELLO, Rafael S.; SERAFIM, Vinícius da S.; WEBER, Raul F. Técnicas de segurança da informação: da teoria à prática. In: CONGRESSO DA SOCIEDADE BRASILEIRA DE COMPUTAÇÃO, 22., 2002, Florianópolis. **Anais...** Florianópolis: ILTC, 2002. p. 129-192.

CERT. (Computer Emergency Response Team) Disponível em: <http://www.cert.org/stats//>. Acesso em 12 de maio 2007.

CERT.BR. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em 12 de maio 2007.

GANGEMI SR., G. T.; LEHTINEN, Rick; RUSSELL, Deborah. **Computer security basics**. 2th ed. Sebastopol: O'Reilly Media, 2006. 310 p. ISBN 0-596-00669-1.

HANSMAN, Simon; HUNT, Ray. A taxonomy of network and computer attacks. **Computers and Security**, v. 24, n. 1, p. 31-43, February, 2005.

KIM, Gene; WARMACK, Rob. Proving control of the infrastructure: the need for independent detective controls within change/configuration management, Portland, Tripwire, 2005.

LANDWEHR, Carl E. Computer security. **International Journal of Information Security**, v. 1, n. 1, p. 3-13, July 2001.

PAPADAKI, Maria et al. A response-oriented taxonomy of it system intrusions. In: PROCEEDINGS OF EUROMEDIA CONFERENCE, 7., 2002, Modena. **Proceedings…** Modena, 2002. p. 87-95.

PFLEEGER, Charles P.; PFLEEGER; Shari Lawrence. **Security in Computing**. 3th ed. Upper Saddle River: Prentice Hall PTR, 2003. 746 p. ISBN 0-13-035548-8.

STALLINGS, William. **Cryptography and network security, principles and practices**. 4th ed. Upper Saddle River: Prentice Hall International, 2006. 680 p. ISBN 0-13-187316-4.

VASIU, Ioana; VASIU, Lucian. Dissecting computer fraud: from definitional issues to a taxonomy. In: INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (HICSS'04), 37, Hawaii, 2004. **Proceedings…** Washington:IEEE, 2004. p. 701-709.

[1] Este artigo deriva da pesquisa realizada pelo Patryck Ramos Martins e seu orientador (Rafael da Rosa Righi) no curso de Pós-Graduação em Gestão da Segurança da Informação em Redes de Computadores do SENAI/SC Florianópolis. A versão completa da pesquisa, contendo a relação completa dos trabalhos relacionados e estudo de caso, pode ser encontrada na biblioteca da instituição.

Originais recebidos em: 12 mar. 2008.
Texto aprovado em: 07 abr. 2008.

SOBRE OS AUTORES

Patryck Ramos Martins

Especialista (Pós Graduação - Lato Sensu) em Gestão da Segurança da Informação em Redes de Computadores, tendo concluído a especialização em novembro de 2007. Ele adquiriu o grau de Bacharel em Ciência da Computação na Universidade do Vale do Itajaí, no princípio do ano de 2005. Atualmente é gerente de redes - Diretoria de Vigilância Epidemiológica. Tem experiência na área de Ciência da Computação, com ênfase em Sistemas de Informação, Redes de Computadores e Segurança Computacional.

E-mail: patryckrm@gmail.com

Rafael da Rosa Righi

Mestre em Ciência da Computação pela Universidade Federal de Santa Catarina (PPGCC-UFSC), tendo concluído o mestrado em fevereiro de 2005. Ele adquiriu o grau de Bacharel em Ciência da Computação na Universidade Federal de Santa Maria (UFSM) no princípio do ano de 2003. Suas áreas de pesquisa são segurança em sistemas distribuídos, proteção de redes Peer-to-Peer, acordos de níveis de serviço (SLA), mecanismos de controle de acesso não tradicionais e infra-estrutura de chaves públicas. Rafael Righi trabalhou junto à equipe do PoP-SC (Ponto de Presença da RNP em Santa Catarina) na segurança das redes UFSC e RCT (Rede Catarinense de Tecnologia) e atualmente exerce a função de professor no ensino superior e pós-graduação na Faculdade de Tecnologia SENAI Florianópolis. Por fim, Rafael também atua como instrutor do Programa Cisco Networking Academy e possui as certificações CCNA, CCAI e CWNA.

E-mail: righi@ctai.senai.br