UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
ENGENHARIA DE COMPUTAÇÃO

BRUNO ANKEN MOROMIZATO ZANINELLO

DETECÇÃO DE ANOMALIAS EM REDES DE COMPUTADORES

TRABALHO DE CONCLUSÃO DE CURSO 1

CORNÉLIO PROCÓPIO

2017

BRUNO ANKEN MOROMIZATO ZANINELLO

DETECÇÃO DE ANOMALIAS EM REDES DE COMPUTADORES

Proposta de Trabalho de Conclusão de Curso apresentada ao curso de Engenharia de Computação da Universidade Tecnológica Federal do Paraná, câmpus Cornélio Procópio, como requisito parcial para a obtenção do título de Bacharel em Engenharia de Computação.

Orientador: Prof. Dr. Lucas Dias Hiera Sampaio

CORNÉLIO PROCÓPIO

2017

Dedico este texto à minha família, que sempre me apoiou de diversas formas em toda a minha trajetória vida.

AGRADECIMENTOS

Agradeço aos meus amigos, sem os quais minha caminhada até este momento certamente teria sido mais árdua, ao meu professor orientador, que me ajudou, apoiou e orientou de maneira impecável neste trabalho e, principalmente, à minha família, sem a qual teria sido impossível chegar a este momento.

RESUMO

ZANINELLO, Bruno Anken Moromizato. DETECÇÃO DE ANOMALIAS EM REDES DE COMPUTADORES. 20 f. Trabalho de Conclusão de Curso 1 – Engenharia de Computação, Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2017.

A segurança em redes de computadores é uma área que movimenta grande quantidade de capital no mercado, desde gastos com reparos de danos causados por ataques efetuados a investimentos em proteções para que os ataques não venham a se concretizar. Os estudos acerca de sistemas de detecção de anomalias iniciaram-se em meados da década de 1980 e foram avançando juntamente às novas tendências tecnológicas na área. Atualmente existem sistemas de detecção de anomalias com arquiteturas distribuídas e atuando na nuvem, por exemplo. A proposta deste trabalho é a criação de um sistema de detecção de anomalias em redes de computadores a partir de uma plataforma ou método de aprendizado de máquina que utilizará um baseline como referência para sua atuação.

Palavras-chave: Detecção de anomalias, Redes de computadores, Segurança.

ABSTRACT

ZANINELLO, Bruno Anken Moromizato. COMPUTER NETWORK ANOMALY DETECTION. 20 f. Trabalho de Conclusão de Curso 1 – Engenharia de Computação, Universidade Tecnológica Federal do Paraná. Cornélio Procópio, 2017.

Computer network security is an area that involves a great amount of money, from damage repairing costs of effective attacks to investments on protection against attacks to come. Studies about anomaly detection systems began in the mid 1980s and advanced alongside the new technological trends in the area. There are, nowadays, anomaly detection systems with distributed architecture and cloud acting ones, for example. The purpose of this work is the creation of a computer network anomaly detection system utilizing a machine learning platform or method that uses a baseline as its reference.

Keywords: Anomaly detection, Computer network, Security.

SUMÁRIO

1 INTRODUÇÃO

O número de dispositivos conectados à internet cresce de forma exponencial atualmente. Desde tecnologias conhecidas que comumente são conectados a uma rede, como computadores, notebooks, celulares e tablets às mais novas invenções e tendências da Internet das Coisas, que adiciona televisões, geladeiras e sensores à rede mundial.

A quantidade cada vez maior de dispostivos com diferentes arquiteturas e tecnologias sendo conectados à internet, bem como a disponibilização de novos e crescentes serviços multimídia, aumentam o tráfego nas redes em que estes dispositivos se encontram e, junto a isso, também aumentam a vulnerabilidade e possibilidade de ataques a estas redes, sejam elas de uso doméstico ou redes cooporativas com enorme volume de tráfego.

A segurança de um ambiente virtual é uma grande necessidade já há vários anos e os ataques a redes de computadores vêm aumentando tanto em números absolutos quanto em sofisticação. Novas técnicas surgem com novas tecnologias e nenhuma rede nem sistema está completamente seguro ou livre de riscos.

Uma reportagem aponta que o gasto com produtos e serviços de segurança da informação seria de 81,6 bilhões de dólares (R$257,85 bilhões) em 2016 (BOUÇAS, 2016). Outra notícia aponta que o gasto seria de 86,4 bilhões de dólares (R$273,02 bilhões) em 2017 e chegaria a 93 bilhões de dólares (R$293,88 bilhões) em 2018 (BRADLEY, 2017).

Estima-se que, em 2017, 445 bilhões de dólares (R$1,4 trilhões) serão gastos anualmente por conta de cibercrimes no mundo, com expectativas de que este valor aumente para 2,1 trilhões de dólares (R$6,64 trilhões) até 2019 (COMPUTERWORLD, 2017). Acredita-se que, só no Brasil, o gasto com crimes virtuais foi de R$35 bilhões em 2016(WALTRICK, 2016).

Uma infecção em massa do ransomware Wannacry, que aconteceu no início do mês de maio de 2017, afetou o atendimento do Instituto Nacional de Segurança Social (INSS) e atingiu empresas e órgãos públicos no Distrito Federal e mais quatorze estados brasileiros (G1, 2017), além de ter se alastrado por cerca de 150 países (CEBRIÁN, 2017),

causando diversos danos a governos e empresas por todo o mundo.

Tendo em vista o grande impacto econômico da área de segurança de computadores no mundo, percebe-se que o estudo e implementação de técnicas, métodos e sistemas de defesa ou prevenção de ataques e infecções torna-se uma necessidade.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 HISTÓRICO ACERCA DE SISTEMAS DE DETECÇÃO DE ANOMALIAS

As pesquisas na área de detecção de anomalias se iniciaram em meados da década de 1980. É evidente que a internet como é conhecida hoje não existia neste período, e os meios de comunicação, protocolos e tecnologias que a originariam ainda estavam sendo propostos.

Um dos primeiros trabalhos nesta área foi de James P. Anderson. Em seu trabalho, Anderson diz que as informações colhidas por auditorias de sistemas na época não eram suficientes para que os profissionais que lidavam com a segurança dos sistemas conseguissem agir da maneira adequada às ameaças presentes. Anderson então propõe aumentar a quantidade de informações coletadas utilizando-se de ferramentas e programas para realizar tal coleta (ANDERSON, 1980).

Estes dados a serem recolhidos seriam frutos de um estudo de como os dados de técnicas de auditoria se manifestam e indicam a ocorrência de ataques ou ameaças. Até então, os meios mais comuns de se detectar algum tipo de intrusão eram através da leitura de logs de auditorias (KEMMERER; VIGNA, 2002). Esta técnica era pouco efetiva, visto que todos os logs eram analisados um a um pelos administradores de sistemas em busca de indícios de violações no sistema.

Em 1986, foi publicado um artigo de Dorothy E. Denning onde ela descreve um modelo para detecção de intrusões em tempo real, tanto de tentativas de ataques externos quanto internos. Dorothy baseou seu modelo na premissa de que o uso anormal de um sistema pode indicar a exploração de vulnerabilidades (DENNING, 1987).

Como o modelo proposto por Denning é independente da plataforma, ambiente ou qualquer sistema ou ameaças específicos, o mesmo tornou-se um framework de propósito geral que inspirou diversos pesquisadores (MCHUGH et al., 2000) e criou a base para os sistemas de detecção de intrusão (Intrusion Detection System, IDS) que viriam a ser

desenvolvidos nos anos seguintes.

Ao longo do final da década de 1980 e ao decorrer da década de 1990, uma máxima continuou verdadeira: nenhum computador ou sistema é livre de vulnerabilidades. Os sistemas podem sofrer tanto ataques internos, como usuários abusando de seus privilégios dentro do sistema, quanto ataques externos, onde usuários não autorizados tentam penetrar no sistema.

Em meados da década de 1990 existiam 5 tipos comuns de IDS: Threshold Detection, Anomaly Detection, Rule-Based Penetration Identification, Model-Based Intrusion Detection e Intrusion Prevention (ILGUN et al., 1995).

A técnica de Threshold Detection (detecção de limite, em traduçãolivre) é a mais rudimentar das cinco, uma vez que ela grava cada ocorrência de um determinado evento e analisa a quantidade de suas ocorrências dentro de um determinado período de tempo. Se estas ocorrências ultrapassarem um certo limite no tempo estabelecido, isto pode indicar a ocorrência de uma intrusão no sistema.

Já a técnica Anomaly Detection (detecção de anomalia) estabelece padrões de uso para cada usuário do sistema. Se o resultado de alguma auditoria de uso do sistema apontar resultados diferentes do padrão esperado de algum usuário, é possível que tenha ocorrido alguma intrusão no sistema.

Um Rule-Based Penetration Identification (identificação de penetração baseado em regras, em tradução livre) é um sistema que, a partir de uma única auditoria de um evento, [e capaz de identificar alguma ameaça ao sistema. Eles também são capazes de identificar indicativos de penetração a partir de uma sequência de eventos suspeitos.

O Model-Based Intrusion Detection (detecção de intrusão baseado em modelo, em tradução livre) tem como objetivo modelar cenários que apresentem comportamentos característicos de uma intrusão. Desta maneira os administradores criam cenaŕios de penetração de maneira abstrata e entregam toda a responsabilidade de determinar quais resultados de auditorias são suspeitos para algum tipo de sistema específico para tal.

Já um sistema que implementa a técnica Intrusion-Prevention (prevenção de intrusão) traz utilidades para o administrador tais como um conjunto de ferramentas que auxilia na busca por vulnerabilidades comumente exploradas por atacantes presentes nas configurações do sistema ou uma abordagem que evite a execução de vírus de computadores ou Cavalos de Tróia dentro do sistema.

No começo dos anos 2000 não existiam sistemas de detecção de intrusão em tempo

real robustos o suficiente para detectar ataques avançados de atacantes bem treinados (BASS, 2000). Um dos defeitos dos mesmos era a grande taxa de falso positivos, que acarretava em grandes perdas financeiras para as empresas que implementavam tais sistemas. Este problema persiste até hoje, conforme relatado por Wagner Rodrigues em sua palestra "Desconstruindo Casos de (in)Segurança da Informação: três décadas... ainda uma jornada".

Outro problema era o gerenciamento de redes, que muitas vezes falhava em prover informações úteis ou relevantes aos profissionais envolvidos na administração ou segurança de redes e sistemas. O gerenciamento da rede e os sistemas de detecção devem trabalhar em conjunto para que os dados possam ser transformados em informações úteis para que o estado da rede possa ser claramente definido e ações corretas e objetivas possam ser tomadas de acordo com cada cenário (BASS, 2000).

De maneira geral, todos os IDS podem ser classificados de acordo com sua premissa em duas categorias: anomaly-based (baseado em anomalia) e signature-based (baseado em assinatura).

Um IDS baseado em anomalia coleta grande quantidade de dados de logs de uso do sistema para traçar perfis de comportamento normais de usuários e atividades do sistema. Baseado nestes perfis de comportamento, o IDS monitora o sistema em busca de desvios dos padrões comportamentais entre os usuários (BOUGHACI et al., 2006).

Já um IDS baseado em assinatura, também chamado de misuse-based (baseado em mau-uso, em tradução livre), utiliza-se de uma base de dados de ataques já conhecidos e estudados para comparar o comportamento do sistema com o desta base de dados em busca de possíveis anomalias (YANG et al., 2010).

Os IDS passaram a ser comumente separados em dois grupos a partir de seus escopos: Host-Based Intrusion Detection System (HIDS, sistema de detecção de intrusão baseado em um hospedeiro em tradução livre) ou Network-Based Intrusion Detection System (NIDS, sistema de detecção de intrusão baseado em rede em tradução livre).

O HIDS atua exclusivamente na máquina em que está instalado, trabalhando com grande proximidade ao sistema operacional da máquina e coletando informações, tais como dados de auditorias ou logs de atividades, utilizadas para identificar possíveis intrusões na máquina de acordo com o uso da mesma (DURST et al., 1999).

Sistemas HIDS conseguem monitorar aplicações específicas nas máquinas em que atuam, algo difícil ou até mesmo impossível em sistemas NIDS. Porém, existe um custo

de desempenho na máquina afetada pelo HIDS, já que seus recursos devem ser utilizados para rodar o HIDS além de realizar sua carga de trabalho (ZHANG et al., 2002).

Já os sistemas NIDS são responsáveis por monitorar atividades de um segmento de rede ou até mesmo da rede inteira, apesar de serem instalados em um único host, assim com o HIDS. Eles analisam o tráfego de pacotes entre os hosts procurando identificar comportamento anormal no formato e dados dos pacotes (DURST et al., 1999).

Sistemas NIDS conseguem monitorar diversos hosts simultaneamente, porém nenhum de maneira aprofundada, e tendem a sofrer problemas de performance, principalmente com grandes velocidades de comunicação na rede. No entanto, a instalação e manutenção de um NIDS é, geralmente, simples e acarreta em custos computacionais quase nulos sobre as máquinas em que atuam (MCHUGH et al., 2000).

Com o avanço e popularização de novas tecnologias e arquiteturas de redes, surgiu um novo modelo de sistema de detecção de intrusões: o Distributed Intrusion Detection System (DIDS, sistema de detecção de intrusão distribuído, em tradução livre). Este sistema analisa as atividades de diversos hosts na rede, sejam estas atividades específicas de cada host ou de segmentos de redes, e faz uma agregação dos mesmos (KANNADIGA; ZULKERNINE, 2005).

A análise dos dados isolados de um único host pode não ser suspeita o suficiente para gerar um alerta dos sistemas HIDS ou NIDS, porém, analisadacotação dólar 6/10 2017cotação dólar 6/10 2017s em conjunto, as atividades podem ser suficientemente anômalas para disparar um alerta de um sistema DIDS.

2.2 TRABALHOS RELACIONADOS

Com regularidade ocorre o surgimento de novas tecnologias e as já existentes estão sempre em um processo de avanços e melhorias. Com o surgimento e evolução de diversas arquiteturas de sistemas, paradigmas computacionais e técnicas de ataques diversas, o mesmo deve ocorrer com as tecnologias de proteção de sistemas.

Em 2005 foi proposta uma ferramenta que se utiliza de aprendizado de máquina para a criação de uma base de dados que não necessita da intervenção humana necessária em um IDS baseados em assinatura (SHON et al., 2005).

A ferramenta utiliza a técnica de Algoritmo Genético para escolher os campos mais apropriados do pacote para utilizar nas análises. Estes campos são então refinados e

passam por um filtro para aumentar a performance da próxima etapa, na qual os dados são enviados para uma versão aprimorada de Support Vector Machine (SVM), um algoritmo que utiliza dois métodos de aprendizado de máquina, um supervisionado e outro não-supervisionado, para classificar os pacotes recebidos como anômalos ou normais.

Em Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes (HWANG et al., 2007) é proposto um NIDS híbrido, baseado tanto em assinatura quanto em anomalia. Desta maneira os autores conseguiram detecções com maior taxa de acurácia e menos alarmes falsos, combinando a baixa taxa de falsos-positivos de um IDS baseado em assinatura com a habilidade de um sistema de detecção de anomalias em detectar novos tipos de ataques.

Já a proposta do trabalho HIDS-DT: An Effective Hybrid Intrusion Detection System Based on Decision Tree (YANG et al., 2010) também é de um sistema híbrido, baseado em assinatura e com detecção de anomalia, visando a descoberta de novos ataques e mantendo uma boa taxa de detecção, e adiciona uma Árvore de Decisão, que é uma tabela de predição comumente usada na área de mineração de dados.

O modelo baseado em assinatura identifica o tipo de protocolo da instância de dados e então escolhe o algoritmo de árvore de decisão mais eficiente para realizar a rotina de detecção. No modelo baseado em detecção de anomalia, as três árvores de decisão que o estudo utiliza são testadas nas instâncias de dados e a mais eficiente é escolhida. Uma instância só é considerada como intrusa apenas quando ambos os modelos a identificarem como uma intrusão.

O trabalho Distributed Cloud Intrusion Detection Model (GUL; HUSSAIN, 2011) propõe um modelo de sistema multi-thread distribuído aplicado à nuvem, alegando que os IDS tradicionais não se adequam de maneira eficiente a um ambiente em nuvem, o qual está sujeito a diversas ameaças de segurança e vulnerabilidades por conta, entre outros fatores, de sua arquitetura distribuída.

Outro fator que impede a implantação na nuvem de IDS tradicionais é que os mesmos não conseguem manipular de maneira eficaz a quantidade massiva de tráfego presente na nuvem, visto que a maior parte dos IDS funciona em uma única thread.

O sistema proposto é distribuído, pois atua tanto como um NIDS quanto como um HIDS simultaneamente, transparente com o usuário e otimizado, visto que envia alertas para os usuáros e entrega informações específicas ao provedor do serviço em nuvem.

Em Behavior Rule Specification-Based Intrusion Detection for Safety Critical

Medical Cyber Physical Systems (MITCHELL; CHEN, 2015) é proposto um sistema de detecção de intrusão baseado em especificação que se utiliza de regras de comportamento esperado de aparelhos em um medical cyber-physical system (MCPS, sistema ciber-físico médico, em tradução livre), onde a segurança do paciente é de extrema importância.

Um IDS baseado em especificação cria uma base através de especificações do programa que descrevem qual o comportamento esperado do programa. O sistema então monitora os programas em execução em busca de desvios de comportamento das especificações. Desta maneira, ataques podem ser detectados mesmo se não houverem detecções dos mesmos anteriormente.

Uma grande diferença entre a modelagem de um IDS aplicado a um MCPS é a relação bem próxima que existe entre as detecções de intrusões e os componentes físicos do sistema médico.

Portanto, ao invés de investigar as rotas dos pacotes ou perdas dos mesmos procurando comportamento anômalo de comunicação, deve-se testar os dados colhidos pelos sensores médicos à procura de manifestações físicas de comportamento anômalo. As regras de comportamento são transformadas em máquina de estados para que uma máquina sob monitoramento possa ter suas transformações de estado facilmente comparadas ao comportamento esperado de tal máquina.

Em Network Anomaly Detection System using Genetic Algorithm and Fuzzy Logic (HAMAMOTO et al., 2018) é proposto um sistema que combina Algoritmo Genético à Lógica Fuzzy para detecção de anomalias em redes. O Algoritmo Genético é utilizado para gerar um Digital Signature of Network Segment (DSNS, assinatura digital de segmento de rede, em tradução livre), que estima o comportamento esperado da rede. Um sistema que se utiliza de Lógica Fuzzy é, então, aplicado ao DSNS para determinar se uma instância representa uma anomalia ou não.

As técnicas de Algoritmo Genético e Lógica Fuzzy são adequadas para lidar com problemas que incluem incertezas, como é o caso de redes de computadores. O sistema proposto funciona de maneira autônoma, aplicando um método padrão aos dados coletados da rede, sem rotulá-los, o que implica em uma técnica de treinamento não-supervisionada.

3 TECNOLOGIAS E FERRAMENTAS

3.1 CARACTERIZAÇÃO DE TRÁFEGO

A caracterização de tráfego de uma rede permite a modelagem de padrões de comportamento em um segmento de rede em relação ao tempo (Jr et al., 2005). Este padrão é conhecido como baseline ou DSNS.

Pode-se definir o DSNS com um conjunto de informações que mostram o perfil de tráfego em um segmento de rede através de picos e vales de volume de tráfego, quantidade de erros, tipos de protocolos e serviçoes que são utilizados pelo dado segmento.

Um DSNS pode ser criado a partir da utilização de diversos protocolos, como em A Methodology for Detection and Estimation of Software Aging (GARG et al., 1998), onde foi utilizado o Simple Network Management Protocol (SNMP), que oferece serviços de gerenciamento de redes, como quantidade de dados trafegados, ou, mais usual atualmente, através de protocolos como o Netflow (CISCO, 2011), um serviço disponível em diversos produtos da companhia Cisco, o IP Flow Information Export (IPFIX) (CLAISE et al., 2013), um protocolo da IETF utilizado para transmitir informações de fluxo de tráfego pela rede e o sFlow (SFLOW.ORG, 2017), uma tecnologia padrão da indústria utilizada para medir o tráfego da rede e coletar, armazenar e analisar os dados advindos desta mensuração.

3.2 HEURÍSTICA

De acordo com Judea Pearl, heurísticas são critérios, métodos ou princípios para decidir qual dentre diversas alternativas tende a ser a mais eficiente para alcançar um determinado objetivo, como o Algoritmo Genético, por exemplo. Atualmente, diversas técnicas de heurísticas são aplicadas nos campos de mineração de dados, aprendizado de máquina e inteligência artificial (PEARL, 1984).

3.3 APRENDIZADO DE MÁQUINA

Segundo SAMUEL, A. L., 1959 apud MUNOZ, A., "aprendizado de máquina é o campo de estudo que dá aos computadores a habilidade de aprender sem ser explicitamente programado". "Atualmente, a área de aprendizado de máquina é uma combinação de diversas outras áreas, como estatística, teoria da informação, teoria de algoritmos, probabilidade e análise funcional"(MUNOZ, 2014).

4 PROPOSTA

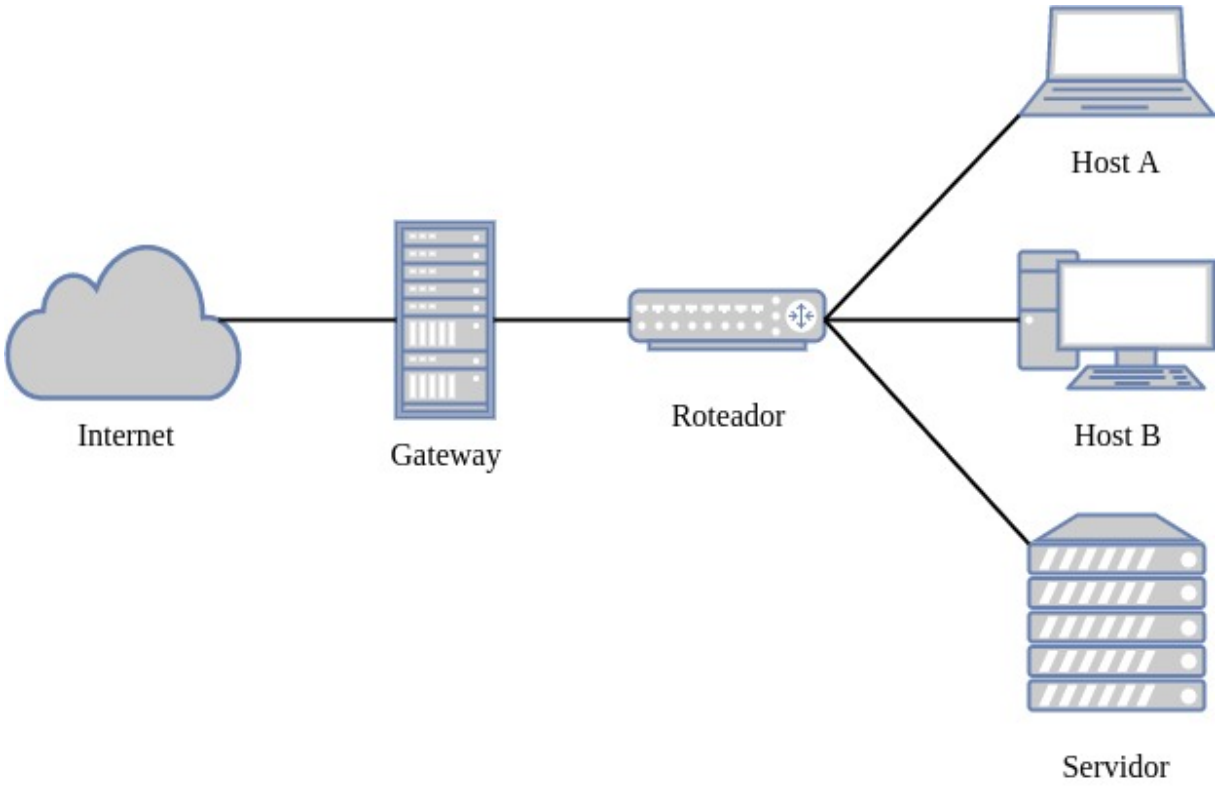

Figura 1: Exemplo de localização de um gateway em uma rede simples.

A proposta deste trabalho é a criação de um sistema de detecção de anomalias em redes de computadores. Para tal, será utilizada uma técnica heurística para a caracterização do tráfego da rede e uma plataforma ou método de aprendizado supervisionado de máquina será treinado para realizar a detecção automática de anomalias na rede.

A análise do tráfego será realizada sobre o gateway, local por onde passam todos os dados que serão enviados para a internet e também todos que são recebidos da mesma. Um esquema simples de uma rede que exemplifica o funcionamento de um gateway pode ser visto na Figura 1.

REFERÊNCIAS

ANDERSON, J. P. **Computer security threat monitoring and surveillance.** Gaithersburg: National Institute of Standards and Technology, 1980.

BASS, T. Intrusion detection systems and multisensor data fusion. **Communications of the ACM**, v. 43, n. 4, p. 99–105, abril 2000.

BOUÇAS, C. Gastos mundiais com segurança da informação atingem US$86,1 bi no ano. **Valor Econômico**, São Paulo, out. 2016. Disponível em: <http://en.wikibooks.org/wiki/LaTeX>. Acesso em: 8 de outubro de 2017.

BOUGHACI, D. et al. Distributed intrusion detection framework based on autonomous and mobile agents. **2006 International Conference on Dependability of Computer Systems**, Poland, p. 248–255, maio 2006.

BRADLEY, T. Gartner predicts information security spending to reach $93 billion in 2018. **Forbes**, Nova Iorque, Estados Unidos da América, ago. 2017. Disponível em: <https://www.forbes.com/sites/tonybradley/2017/08/17/gartner-predicts-information-security-spending-to-reach-93-billion-in-2018/6625c0633e7f>. Acesso em: 8 de outubro de 2017.

CEBRIÁN, B. D. Cibertaque: o vírus wannacry e a ameaça de uma nova onda de infecções. **El País**, Madri, Espanha, mai. 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/05/14/internacional/1494758068_707857.html>. Acesso em: 8 de outubro de 2017.

CISCO. **NetFlow Version 9 Flow-Record Format**. Mai. 2011. Disponível em: <https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html>. Acesso em: 9 de outubro de 2017.

CLAISE, B.; TRAMMELL, B.; AITKEN, P. **Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information**. IETF: [s.n.], Set. 2013. Disponível em: <https://tools.ietf.org/html/rfc7011>. Acesso em: 9 de outubro de 2017.

COMPUTERWORLD. Gastos globais com seguros contra ataques cibernéticos já somam cerca de US$ 2 bi. **COMPUTERWORLD**, São Paulo, fev. 2017. Disponível em: <http://computerworld.com.br/gastos-globais-com-seguros-contra-ataques-ciberneticos-ja-somam-cerca-de-us-2-bi>. Acesso em: 8 de outubro de 2017.

DENNING, D. E. An intrusion-detection model. **IEEE Transactions on Software Engineering**, IEEE, p. 118–131, fevereiro 1987.

DURST, R. et al. Testing and evaluating computer intrusion detection systems. **Communications of the ACM**, v. 42, n. 7, p. 53–61, julho 1999.

G1. Ciberataques em larga escala atingem empresas no mundo e afetam brasil. **G1**, Rio de Janeiro, mai. 2017. Disponível em: <https://g1.globo.com/tecnologia/noticia/hospitais-publicos-na-inglaterra-sao-alvo-cyber-ataques-em-larga-escala.ghtml>. Acesso em: 8 de outubro de 2017.

GARG, S. et al. A methodology for detection and estimation of software aging. **Proceedings Ninth International Symposium on Software Reliability Engineering**, Alemanha, p. 283–292, novembro 1998.

GUL, I.; HUSSAIN, M. Distributed cloud intrusion detection model. **International Journal of Advanced Science and Technology**, v. 34, p. 71–82, setembro 2011.

HAMAMOTO, A. H. et al. Network anomaly detection system using genetic algorithm and fuzzy logic. **Expert Systems with Applications**, v. 92, p. 390–402, 2018.

HWANG, K. et al. Hybrid intrusion detection with weighted signature generation over anomalous internet episodes. **IEEE Transactions on Dependable and Secure Computing**, v. 4, n. 1, p. 41–55, fevereiro 2007.

ILGUN, K.; KEMMERER, R. A.; PORRAS, P. A. State transition analysis: a rule-based intrusion detection approach. **IEEE Transactions on Software Engineering**, v. 21, n. 3, p. 181–199, março 1995.

Jr, M. L. P.; ZARPELÃO, B. B.; MENDES, L. S. Anomaly detection for network servers using digital signature of network segment. **Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop (AICT/SAPIR/ELETE'05)**, Portugal, p. 290–295, julho 2005.

KANNADIGA, P.; ZULKERNINE, M. Didma: a distributed intrusion detection system using mobile agents. **Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Network**, Estados Unidos da América, p. 238–245, maio 2005.

KEMMERER, R. A.; VIGNA, G. Intrusion detection: A brief history and overview. **Security & Privacy**, Computer, University of Californa Santa Barbara, Goleta, Califórnia, Estados Unidos da América, v. 35, p. 27–30, agosto 2002.

MCHUGH, J.; CHRISTIE, A.; ALLEN, J. Defending yourself: The role of intrusion detection systems. **IEEE Software**, IEEE, v. 17, n. 5, p. 42–51, outubro 2000.

MITCHELL, R.; CHEN, I.-R. Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems. **IEEE Transactions on Dependable and Secure Computing**, v. 12, n. 1, p. 16–30, fevereiro 2015.

MUNOZ, A. **Machine Learning and Optimization**. Nova Iorque, Estados Unidos da América: Courant Institute of Mathematical Sciences, 2014. Disponível em: <https://www.cims.nyu.edu/ munoz/files/ml_optimization.pdf>. Acesso em: 9 de outubro de 2017.

PEARL, J. **Intelligent Search Strategies for Computer Problem Solving**. Estados Unidos da América: Addison-Wesley Publishing Company, 1984.

SFLOW.ORG. **About sFlow**. 2017. Disponível em: <http://www.sflow.org/about/index.php>. Acesso em: 9 de outubro de 2017.

SHON, T. et al. A machine learning framework for network anomaly detection using svm and ga. **Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop**, Estados Unidos da América, p. 176–183, agosto 2005.

WALTRICK, R. Crimes virtuais trazem prejuízo bilionário para brasileiros. **Gazeta do Povo**, Curitiba, nov. 2016. Disponível em: <http://www.gazetadopovo.com.br/economia/inteligencia-artificial/crimes-virtuais-trazem-prejuizo-bilionario-para-brasileiros-c50g4ta0o4u4dwvt7l9ippivh>. Acesso em: 8 de outubro de 2017.

YANG, J. et al. Hids-dt: An effective hybrid intrusion detection system based on decision tree. **2010 International Conference on Communications and Mobile Computing**, China, p. 70–75, abril 2010.

ZHANG, X. et al. Secure coprocessor-based intrusion detection. **EW 10 Proceedings of the 10th workshop on ACM SIGOPS European workshop**, França, p. 239–242, julho 2002.