A ANÁLISE DAS AMEAÇAS POR MEIO DA AUDITORIA DE LOG NATIVO DO SISTEMA E QUAIS AS RAZÕES QUE DIFICULTAM SUA ADOÇÃO

ANALYSIS OF THREATS THROUGH THE NATIVE SYSTEM AUDIT AUDIT AND WHAT REASONS WHY IT IS DIFFICULT FOR THEIR ADOPTION

RODRIGO P. DE FREITAS
Graduado em Tecnologia em Rede de computadores - Faculdade Anhanguera de Anápolis e Especialista em Gestão e Segurança em Redes de Computadores, Universidade Estadual de Goiás (UEG), Campus de Trindade
rodrigo.freitas111@gmail.com

ANTÔNIO CRUVINEL BORGES NETO
Mestre em Engenharia Agrícola e docente da Universidade Estadual de Goiás (UEG) - Campus de Ciências Exatas e Tecnológicas Henrique Santillo (Anápolis - GO) e diretor educacional da Universidade Estadual de Goiás (UEG), Campus de Trindade
antonio@cruvinel.com.br

Resumo: A cada instante, novas tecnologias são lançadas trazendo novos pensamentos, estratégias e culturas. No entanto além dos benefícios gerados pela tecnologia criam-se também novas ameaças com alto potencial de complexidade em relação às existentes. Uma ameaça de alta complexidade possui o mesmo princípio para o seu combate, que é a análise e auditoria de log e que o simples fato de ausência de monitoração os logs aumenta a possibilidade de ameaças simples passarem despercebidas pelos administradores.
Palavras-chave: Segurança da informação. Análise e auditoria de log. Detecção de Ameaças.

Abstract: Every moment, new technologies are launched bringing new thoughts, strategies andcultures. Besides of the benefits, we also have new threats that increase the complexitythe ones that already existed. However a threat of high complexity has the sameprinciple for its combat, which is the analysis for log audit.The simple fact of not monitoring the logs increases possibilities of simple threats goingunnoticed by the administrators.
Keywords: Information security. Analysis and audit of log. Detection of threat.

INTRODUÇÃO

Atualmente, a informação é considerada um ativo de grande importância que demanda segurança. Para Rodriguez e Silva (2014, p. 2) “A necessidade de manter as informações seguras surgiu com o crescimento da tecnologia, o que ocasionou vazamentos de dados e informações.”. Com o avanço tecnológico, surgem novas ameaças e de maior complexidade

contra a informação. Este trabalho está centrado na norma ISO/IEC 27002:2005 (ABNT, 2005), onde define a importância de registrar e monitorar constantemente os logs da informação, utilizando-se de processos como análise e auditoria.

O artigo tem como objetivo demonstrar que o estudo do log padrão do sistema é necessário para se obter resultados que facilitam a identificação de ameaças.

O mesmo busca verificar também se o estudo do log está sendo utilizado e pesquisado no Brasil, e demonstrar possíveis problemas que dificulta a utilização de análise e auditoria de log. As ferramentas utilizadas para demonstrar os logs coletados são: VIM (Vi improved), Log Analyzer e Ntopng, com o propósito de identificar ameaças.

1. DEFINIÇÕES

Para se criar um ambiente onde podemos incluir a análise e auditoria de log como mecanismo de detecção de ameaças é importante ter em mente o que venham a ser a informação, e o que é uma ameaça contra a informação.

1.1. INFORMAÇÃO

De uma forma simplista a informação é tudo aquilo que pode gerar algum conhecimento. No entanto Silva e Coelho (2013) vão um pouco além, dizendo que, todo conjunto organizado de dados pode ser considerado uma informação.

1.2. AMEAÇAS

Para Coelho, Araújo e Bezerra (2014, p. 3) “Ameaça é qualquer evento que explore vulnerabilidade.” Qualquer tipo de ação que venha transgredir as normas definidas pela instituição de forma intencional ou acidental deve ser consideradouma ameaça.

1.3. SEGURANÇA DA INFORMAÇÃO

As definições mínimas de proteção da informação no Brasil são determinadas pela ABNT, em normas como ISO/IEC 27002:2005 (ABNT, 2005) e descrevem que “A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de

software e hardware.”

2. O ESTUDO DO LOG

O log é uma informação preciosa que define um evento como uma ocorrência.

Para Bhagyasheree e Ambarish (2012) os logs são recursos inestimáveis para detecção de ataques. De acordo com Edson e Figueiredo (2001) os cracks são considerados tão importantes que a primeira lição necessária ao aprendizado da tecnologia da informação é como eliminar seus rastros registrados pelos logs. Para Shostack e Stewart (2008) um analista brilhante sem dados é um sábio porque criar um gerenciamento de log é fundamental para entender a natureza do problema.

2.1. TIPOS DE LOGS

Para inicializar a coleta e o estudo do log (figura 1) é importante entender as fontes destes dados, uma vez que se recebem dados tanto de hardware como software. Trabalhar com os logs diretamente da fonte, sem relacioná-los com outras fontes, podem gerar informações falhas e aumentar a dificuldade na resolução de problemas. Pensando nisso propõem-se um modelo de categorização dos logs que reúne informações similares e relaciona suas categorias entre as diferentes fontes.

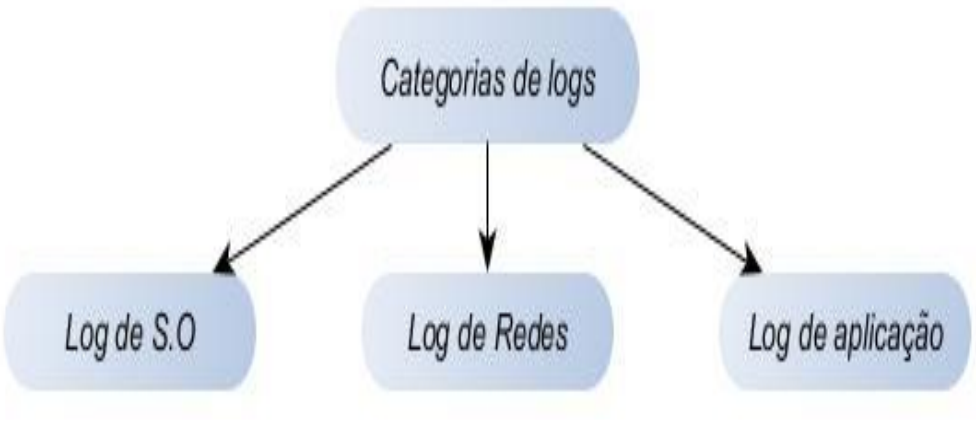

Figura 1: Categorias de Log. Fonte: Autores (2016)

Na figura 1, é proposto um modelo simples de 3 categorias, no qual os logs de sistema operacional (S.O) contém informações de um S.O como Linux, Hypervisor e logs de redes,

temos informações de switch, roteadores ou algum software ligado com o tráfego de rede. E ainda logs de aplicações que extraem informações de software como “Domain name sytem” (DNS), e-mail e outros.

2.2. O CICLO DA ANÁLISE E AUDITORIA DE LOG

A análise e auditoria de log possuem um ciclo de vida. Söderström e Moradian (2013) destacamque uma auditoria é um sistema de processo interminável, que envolvem duas etapas: registro e auditoria. O processo em duas etapas possui algumas falhas que podem levar ao descrédito do log. Desta forma propõem-se um ciclo de quatro etapas com a inclusão de análise e monitoramento dos registros, representado pela figura 2.

Figura 2: Ciclo de Auditoria. Fonte: Autores (2016)

O ciclo proposto visa evitar o desperdício de tempo com auditoria de informações irrelevantes que comprometem os resultados.

a) Registro

Para Söderström e Moradian (2013) o registro é a coleta de dados de acordo com sistema ou configuração de parâmetros. Nesta etapa registram-se todos os eventos de

hardware e software sem se preocupar com a qualidade dos registros.

b) Análise

Para Maicon (2009) a seleção dos principais componentes de um registro baseado nas necessidadesde negócio, é obter informações de estado dos sistemas com o cruzamento de métricas.

Neste momento é descartado tudo que não tem relevância para auditoria e um plano de retenção é definido de acordo com sua importância.

c) Monitoramento

Segundo Maicon (2009) a verificação contínua das informações selecionadas pode trazer uma série de vantagens e permitir que o administrador antecipe eventos que podem comprometer a disponibilidade e integridade do sistema.

Neste momento, é possível perceber se a seleção foi muito profunda, deixando de registrar informação importante, como também propor novas mudanças para melhorar o processo anterior.

d) Auditoria

O termo auditoria é definido como a certificação dos registroscontábeis. Segundo Araújo (2004, p. 13) “É simplesmente a comparação imparcialentre o fato concreto e o desejado”. A auditoria verifica se os processos definidosestão em conformidade com as informações auditadas.

2.3. FORMA DE REGISTRO DE LOG

Os logs podem ser registrados, de forma local, nos dispositivos, no entanto mais suscetíveis a alguma invasão e podem sofrer alterações. Para Azevedo et al. (2011) oconceito consiste em definir um servidor que receba e armazene todos os logs, tantode hardware como de Software, para conseguira auditoria e a proteção. A figura 3 apresenta o ambiente de um CLS onde o NOC relata problema ao SOC e vice-versa.

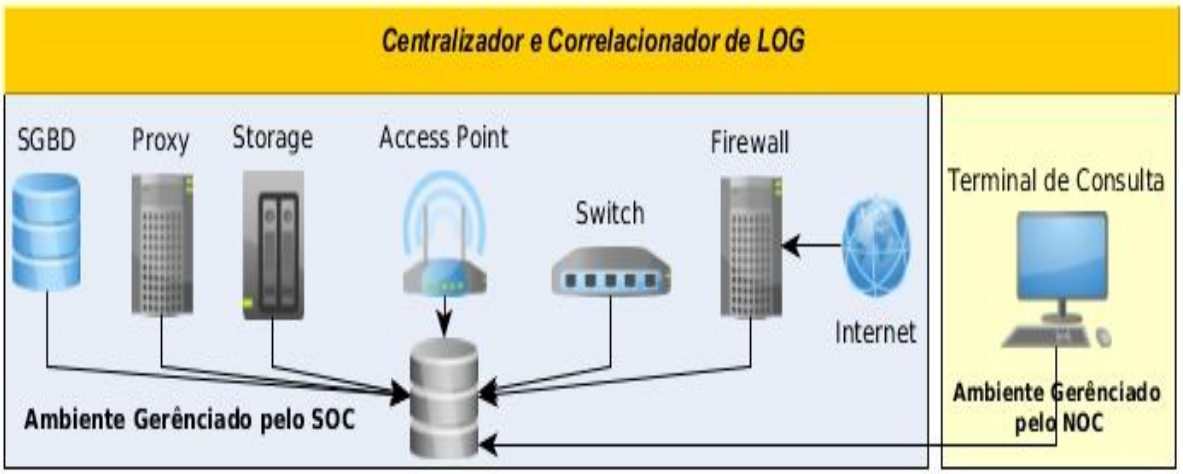

Figura 3: Centralizador de Log. Fonte: Autores (2016)

Com a utilização de um CLS têm-se a possibilidade de desfrutar de uma estratégia cruzada implementando uma Network Operations Center (NOC), que é um usuário das informações armazenadas pelo CLS e um Security Operations Center (SOC), que fica responsável pela administração do CLS.

2.4. O ESTUDO DE LOG NO BRASIL

Em 1997 O Comitê Gestor da Internet (CGI) criou-se Centro de Estudospara Reposta e Tratamento de Incidentes em Computadores (CERT. br) que publicouboas práticas sobre uso de log. Temos ainda norma ISO/IEC 17799/2005, publicadaem sua primeira versão no ano 2000 e atualizado para 27002/2005 no ano de 2007onde define em suas diretrizes a importância do registro dos eventos de logs e suamanutenção para futuras investigações. Atualmente o gerenciamento de log é previstono Marco Civil da Internet (Lei no 12.965, de 23 de abril de 2014) e em recomendações,como da Anatel (Resolução nº 614, de 28 de maio de 2013), que buscam incentivar autilização de log.

Mesmo com mais de 20 anos das recomendações publicadas, o Brasilregistra altos índices de aumento de incidentes de segurança da informação. A 18º pesquisa Global de segurança da informação 2015 realizada pela PwC mostra queem 2015 o Brasil teve um aumento de 274% de incidentes e um prejuízo médio de R$2,4 milhões ao ano. O Brasil ainda tem muito a crescer na área de segurança dainformação onde o estudo do log pode ser considerado um dos primeiros passos.

3. ESTUDO DE CASO

Neste estudo de caso será apresentado logs que foram coletados em umambiente de teste para identificarmos algumas de ameaças. Os logs escolhidostiveramcomo base as estatísticas de incidentes reportados ao cert. br no ano de 2015, onde 54,17% está relacionado a scan port, 3,51% à ataque DoS e 0,34% a invasão desistema, as três juntas temos quase 60% de todas as ameaças notificas no Brasil.

A figura 4 apresenta os logs coletados de um Firewall de borda, com váriasrequisições chegando do mesmo protocolo de internet (IP). Nas linhas em destaquetemos o IP de origem e destino, tempo de vida do pacote (TTL “Time to live”) e odestino final do pacote, identificado pelas portas destino (DPT “Destination Port”).

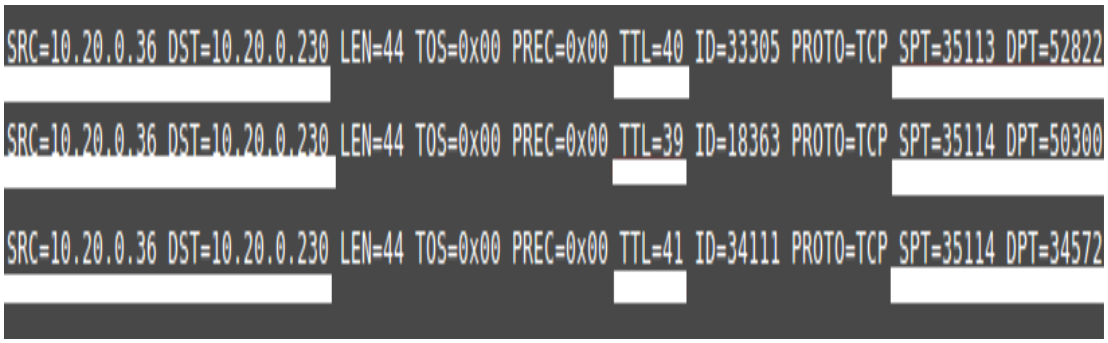

Figura 4: Log firewall de borda visualizado pelo VIM. Fonte: Autores (2016).

A partir das informações deduzimos que o IP de origem 10.20.0.36 está realizando um scan port no IP de destino 10.20.0.230 buscando encontrar todos os serviços hospedados. O TTL é a informação chave, pois se altera em 1 salto, alterando também a porta de destino (figura 5).

Figura 5: Log relacionado entre S.O e aplicação.

Figura 6: Log relacionado entre S.O e aplicação. Fonte: Autores (2016).

Na figura 5 temos Log Analyzer, relacionando os logs de S.O com aaplicação de acesso remoto Secure Shell (SSH). O sistema operacional informa que o IP 10.20.0.36tentou acessar remotamente através da aplicação utilizando o usuário ROOT, comvárias senhas sem obter sucesso. Esta informação é comprovada pelo parâmetroFailed. Caso o atacante descubra a senha, a aplicação informa que o usuárionão tem permissão de acesso remoto pelo parâmetro ilegal user root from, evitandouma invasão por acesso remoto.

Utilizando do ntopng open source pode demonstrar um fluxo de dadoschegando ao servidor web com vários fluxos de um mesmo Log.

Relacionado entre Sistema Operacional e aplicaçãoendereço IP de origem 1.2.3.4, para o protocolo HTTPS3 na mesma faixa de tempo conforme figura 6.

Figura 7: Registro de fluxo ntopng

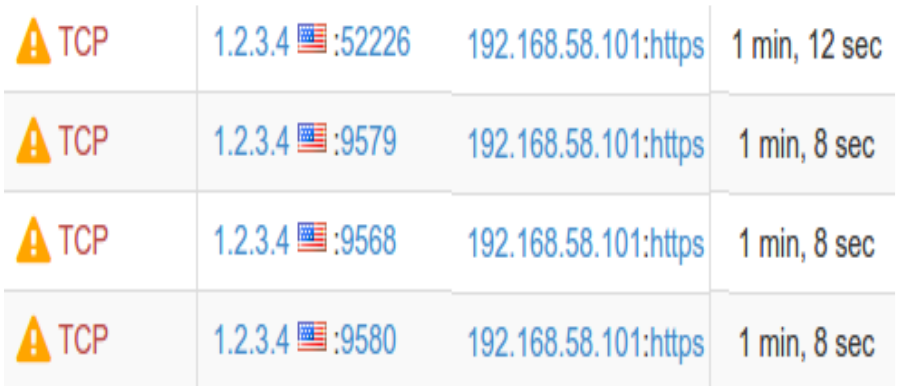

Figura 8: Registro de fluxo ntopng. Fonte: Autores (2016).

Existe a posse da identificação do número de sistema autônomo (ASN) que identificaa origem dos fluxos e a quantidade de dados gerados nos dois sentidos upload e download (figura 7).

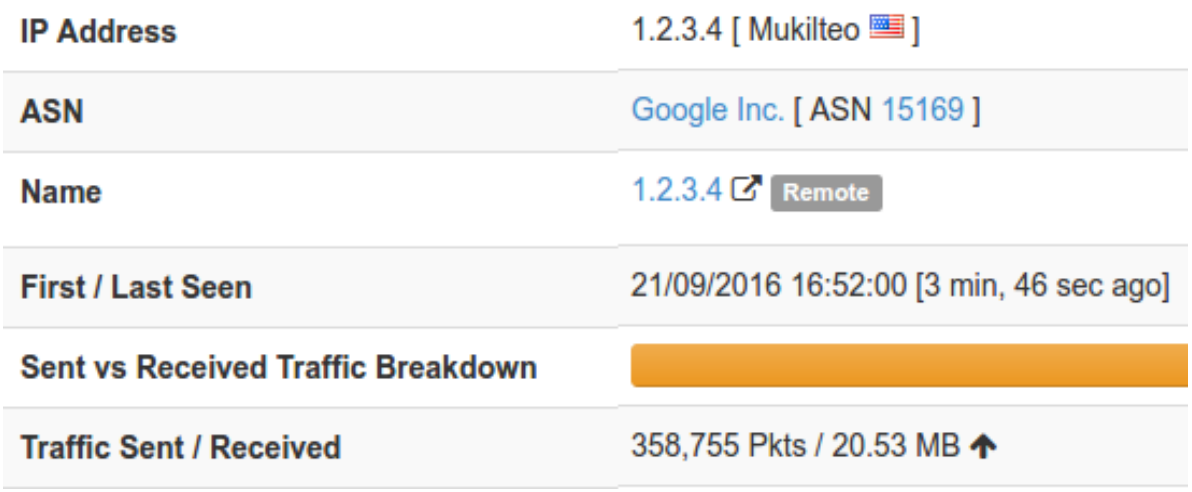

Figura 9: Registro de Fluxo ntopng. Fonte: Autores (2016)

Conforme figura 7 é possível mapear este fluxo como um tipo de ataque de negação de serviço (DoS), por temos vários acesso de um único endereço IP com carga de 20,53 MB/s de dados enviado por um período de 4 minutos.

4. FATORES QUE DIFICULTAM O USO DE LOG

A falta de uma cultura de segurança dificulta o uso de análise e auditoriade log. Ana Helena e Cristiana (2013) ressaltam que implementar uma cultura desegurança da informação é cada vez mais imprescindível. Alguns motivos pela sua falta estãoligadosa ausência de uma política de segurança da informação e ao métodocomo são adquiridas novas tecnologias. Shostack e Stewart (2008) afirmam que écomum o mercado da segurança da informação adquirir nova tecnologia baseadaapenas nas indicações de fabricantes, o que pode gerar uma segurança ineficiente. Ofato é que muitos fabricantes não têm interesse em estimular a implementação deprocessos de segurança, que propicia o entendimento do ambiente de TI. Shostack eStewart (2008) concluem que “A maioria das empresas ganhariam mais se tivessem umentendimento preciso e atualizado do que criaram”.

Uma pesquisa realizada pelo CGI em 2013 mostra que 15% dos órgãosbrasileiros não

possuem uma Política de segurança da informação (PSI) apesar do decreto nº 3.505 de 13 de junho de 2000 instituem a política de segurança da informaçãonos órgãos e entidades da administração pública federal. Uma pesquisa realizada porJunior (2014) nos anais da ANPAD, entre o ano de 2004 a 2013, mostra que o temasegurança da informação teve pouca relevância com apenas 67 artigospublicados com este foco. As duas informações demonstram que o Brasil estácaminhando a passos lentos na segurança da informação, pois as poucas obras referentes ao assunto doutrinamas organizações a não utilizar políticas que podem resguardar a informação.A partir do trabalho apresentado por Junior (2014), foi realizada uma pesquisa nos periódico da base de dados CAPES com o idioma português, entre operíodo de 2006 a 2016 com o foco nos mesmos temas. O resultado da nova pesquisanão foi muito diferente, apresentando 61 artigos com o foco principal em segurançada informação.

5. CONCLUSÃO

Como todo acesso a informação gera um rastro, é possível então criar um ambiente de monitoramento e estabelecer um perímetro de segurança em sua volta.A partir da análise e auditoria de log gerado pela informação, pode-se identificar vários tipos de ameaças bem como e correlacionar várias informações advindas de outras fontes,utilizando-se um CLS de forma proativa e assim evitando ataques futuros.

O Brasil possui recomendações há bastante as quais definem boas práticas com relação ao uso da análise e auditoria de log. Entretanto matéria só foi legislada em 2014, dirigindo assim as empresas a utilizarem de tecnologias de logs. Uma realidade das grandes empresas no Brasil que possui uma cultura de segurança como parte do negócio e utiliza o log como uma forma de agregar valor ao seu produto final.

Contudo,ainda falta estudo e pesquisa sobre como utilizar o rastro deixado pela informação em favor da organização.

A análise e a auditoria de log têm um papel importante na identificação de ameaças, e contribui para entender melhor o ambiente de TI. O seu uso está atrelado a uma cultura de segurança interna, que não e adquirida com a compra de novas tecnologias. Na verdade, as aquisições podem até piorar essa realidade por não incentivar o conhecimento do ambiente e nem a implementação de uma política de segurança da informação (figura 8).

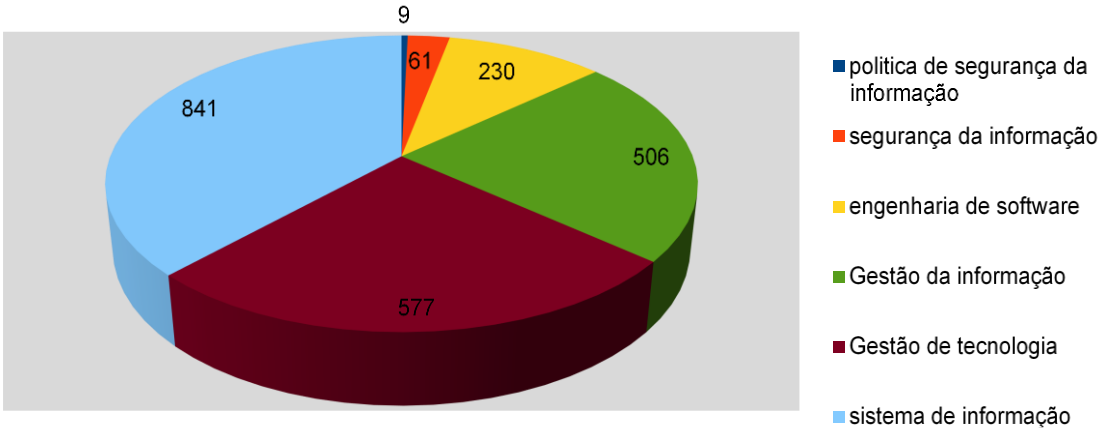

Figura 10: Pesquisa por tema no período entre 2006 a 2016. Fonte: Autores (2016).

Para trabalhos futuros sugere-se que seja criada uma PSI, alinhada a análisee auditoria de log, que definirá os tipos de registro baseado nas necessidades daorganização, e, ainda a criação de categorias como forma de armazenamento. Dessa forma, possibilita a realização de auditoria das informações, agregando valor ao produto final, com auxílio natomada de decisão.

REFERÊNCIAS

ALVES, Maicon M. **Linux Performance& Monitoramento**. Rio de Janeiro: Brasport, 2009.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISSO/IEC 27002:2005: **Tecnologia da informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

AUTOR ANÔNIMO. **SEGURANÇA MÁXIMA**. Tradução Edson Furmankiewic. E, Figueiredo, S. 3. Ed. Rio de Janeiro: Editora: Campus, 2001. p. 194 a 198.

AZEVEDO, M. T.; Pegetti, A. L.; Santos, K. M**. Técnicas de Perícia Forense como Ferramentas de Prevenção de Incidentes de Segurança**. Periódicos de Divulgação Científica da FALS ano V, nº XII DEZ/2011.

BRASIL. **centro de estudos, resposta e tratamento de incidentes de segurança no Brasil – cert.br. Estatísticas sobre notificação de incidentes: Incidentes Reportados**. Disponível em: <http://www.cert.br/stats/ incidentes/2015-jan-dec/tipos- ataque.html>. Acesso em 15 nov. 2016.

COELHO, Flávia E. S.; ARAÚJO, Luiz G. S.; BEZERRA, Edson K. **Gestão da Segurança da Informação NBR 27001 e NBR27002**. Rio de Janeiro: Escola Superior de Redes, 2014.
DEOKAR, Bhagyasheree; HAZARNIS, Ambarish. Intrusion Detection System Using Log Files and Reinforcement Learning.Revista international journal of computer applications, mumbai, Vol 45-no 19, Maio, 2012.

FERNANDES, Jorge Henrique 7.C; SOUZA, Raul Carvalho. **Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais**. Revista brazilian journal of information studies: research trends, Marília, SP, v. 10, n. 1, p.63-75, 2016.

JUNIOR, Antônio Eduardo A; SANTOS, Ernani Marques. **Produção científica sobre segurança da informação em eventos brasileiros.** In: INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS AND TECHNOLOGY MANAGEMENT – CONTECSI, 11. 2014. São Paulo. Proceedings. São Paulo: CONTECSI, 2014. p. 2085-2103.

OLOF, Söderström; ESMIRALDA, Moradian. Secure Audit Log Management. In: **INTERNATIONAL CONFERENCE IN KNOWLEDGE BASED AND INTELLIGENT INFORMATION AND ENGINEERING SYSTEMS-KES2013**, 17.2013. Suécia: Elsevier B. V. 2013. p. 1249-1258.

PINHEIRO, J. M. S.**Os Benefícios da Política de Segurança Baseada na Avaliação de Riscos e na Integração de Ferramentas**. Cadernos Unifoa. Volta Redonda, ano II, n. 4, agosto. 2007. Disponível em: <http://www.unifoa.edu.br/pesquisa/caderno/edição/04/28. pdf>.PwC. 18º EDIÇÃO ANUAL DA PESQUISA GLOBAL DE SEGURANÇA DA INFORMAÇÃO, 2015. Acesso em: 09 nov.2016.

SANTOS, Mauro Tapajós et al. **Gerência de redes de Computadores**. Rio de Janeiro: Escola Superior de Redes, 2015, p. 175-205.

SILVA, Ana Helena E, Coelho, Cristiana Raquel. **Segurança da Informação nas Organizações**. 2012/2013. 252 f. Dissertação (Mestrado em Ciência da Informação) Faculdade de Engenharia Universidade do Porto FEUP, Porto: 2012/2013.

SHOSTACK, Adam; Stewart, Andrew. **A Nova Escola da Segurança da Informação**. Rio de Janeiro: Altos Books, 2008.

TIC GOVERNO ELETRÔNICO 2013**. Pesquisa sobre o uso das tecnologias da informação e comunicação no setor público brasileiro.**2013**.** São Paulo: Comitê Gestor da Internet no Brasil, 2014.