ISSN 0798 1015

REVISTA ESPACIOS

HOME Revista ESPACIOS ÍNDICES A LOS AUTORES

Vol. 38 (Nº 19) Año 2017. Pág. 30

Segurança de informação e a gestão unificada contra ameaças – Um levantamento exploratório

Information security and unified threat management - An exploratory survey

Manassés VICENTE 1

Recibido: 10/11/16 • Aprobado: 10/12/2016

Conteúdo

RESUMO:

O problema de segurança da informação tem recebido pouca atenção nas micro e pequenas empresas no Brasil. A busca pela sobrevivência no mercado muitas vezes faz com que as empresas cortem custos com segurança. Este trabalho é um levantamento exploratório sobre Sistema de Informação (SI) com ênfase em Gestão Unificada Contra Ameaças ou Unified Threat Management (UTM).
Palavras-chave: Sistema de Informação; Segurança da Informação; UTM; Firewall; Endian.

ABSTRACT:

The information security problem has received little attention in micro and small companies in Brazil. The quest for survival in the marketplace often causes businesses to cut costs safely. This work is an exploratory survey on Information Systems (IS) with an emphasis on Unified Threat Management (UTM).
Keywords: Information Systems; Information Security; UTM; Firewall; Endian.

1. Introdução

Este artigo tem como premissa a existência do risco em qualquer situação do cotidiano humano, em maior ou menor grau, e da ausência da segurança absoluta, valendo-se da literatura de espionagem ou contraespionagem. Assume-se como sentença válida para qualquer área, quer seja segurança física, patrimonial, digital da informação, tendo seu ápice na "*espionagem*" ou serviços de inteligência desenvolvidos pelas agências de países como: *Central Intelligence Agency* (CIA); *Federal'naya Sluzhba Bezopasnosti Rossiyskoi Federatsii* (FSB) em tradução livre Serviço Federal de Segurança da Federação Russa sucessora da KGB; *ha-Mossad*

le-Modiin ule-Tafkidim Meyuhadim (MOSSAD) ou Instituto para Inteligência e Operações Especiais de Israel; e, Agência Brasileira de Inteligência (ABIN), entre outros.

É notório que essas agências de inteligência são treinadas para isso e que usam tecnologia de ponta. Em uma entrevista concedida (Gobo, Dossiê Globo News, 2014) o ex-agente da CIA expõe a insegurança na telefonia e na computação, mencionando inclusive o TEMPEST.

O TEMPEST é um codinome para os estudos de comprometimento de emissões de sinais de energia (elétrica, mecânica ou acústica) por qualquer equipamento de processamento de informações, que se interceptados e analisados, pode levar a recuperação do texto original, uma vez que tais sinais de energia podem ser propagados através do espaço e de condutores próximos, conforme tem demonstrado os testes de laboratório e de campo (LASEC/EPFL, 2009).

Saindo do contexto segurança no sentido amplo, e situando o problema da espionagem realizada por empresas em projetos de pesquisa altamente sigilosos, onde patentes de produtos estão envolvidos. Ou ainda casos onde o interesse de compra de um ativo, é motivo da quebra de sigilo ilegalmente, e outros de cunho "*ideológicos*", e que fazem parte do cotidiano brasileiro.

Alguns agentes de agências de inteligência, quando se aposentam começam a trabalhar atendendo a interesses particulares, de empresas e corporações, como observa-se no caso Carlinhos Cachoeira o envolvimento do ex agente da ABIN em (Jornal do Brasil, 2012).

> O ex-funcionário da Agência Brasileira de Inteligência (Abin) Jairo Martins de Souza, citado nos documentos da Operação Monte Carlo, deflagrada pela Polícia Federal para desarticular a quadrilha do bicheiro Carlinhos Cachoeira - responsável pela exploração de máquinas caça-niqueis em Goiás, foi nomeado para o órgão em 1993 e permaneceu até 2000.
>
> O Ministério Público o acusa de ter recebido cerca de R$ 5 mil mensais para convencer policiais a se juntarem à organização criminosa. As investigações apontam que foram pagas propinas a políciais civis, militares, federais, rodoviários e até funcionários do Judiciário, que colaboravam no repasse de informações sobre operações que pudessem prejudicar o interesse do grupo. Entre eles estavam o corregedor-geral da Secretaria de Segurança Pública e Justiça de Goiás, Aredes Correia Pires, e o delegado da Polícia Federal Fernando Byron.

No desenvolvimento deste artigo será realizado um levantamento exploratório sobre a segurança da informação nos órgãos do governo brasileiro, nas empresas brasileiras. Uma abordagem dos mecanismos nas empresas de médio e grande porte, e a falta de mecanismos nas empresas de micro e pequeno porte. Finalizando com a visão do *firewall* e a segurança da informação e o UTM Endian.

---

2. Desenvolvimento

2.1. Órgãos do Governo e Empresas brasileiras - Segurança da Informação

O grupo hacker Fail Shell atacou o site do Instituto Brasileiro de Geografia e Estatística (IBGE) segundo (Jornal do Brasil, 2011):

> IBGE é atacado por grupo paralelo
>
> Hackers do grupo Fail Shell, rival do LulzSec, invadiram o site do Instituto Brasileiro de Geografia e Estatística (IBGE) na madrugada desta sexta-feira. A mensagem: "IBGE Hackeado - Fail Shell" foi exibida no topo da página. O site permanecia fora do ar e com a mensagem dos hackers por volta das 5h.

> Os hackers afirmaram em mensagem na página do IBGE que a invasão é "uma forma de protesto de um grupo nacionalista".

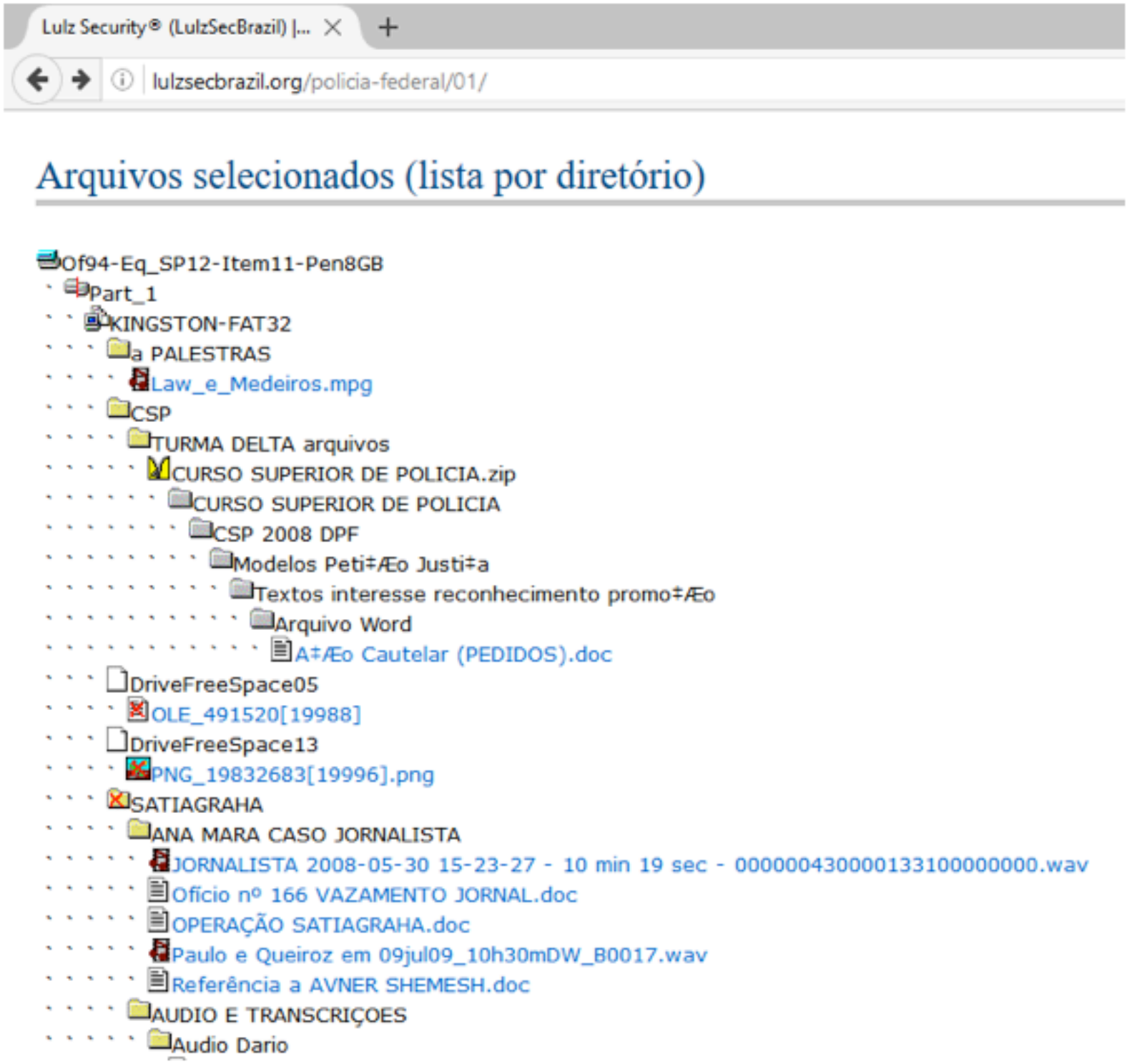
Um dos célebres casos brasileiros é do banqueiro Daniel Dantas do banco Opportunity, investigado pela polícia federal por espionagem. Neste caso a Justiça Federal absolveu Dantas no caso Kroll de acordo com (Jornal O Estado de São Paulo, 2012):

> O banqueiro Daniel Dantas, do Opportunity, e mais dez pessoas foram absolvidas da acusação de formação de quadrilha na Operação Chacal, investigação da Polícia Federal em 2004 envolvendo a Kroll Associates em espionagem. A juíza Adriana Freisleben de Zanetti, da 5.ª Vara Federal Criminal de São Paulo, condenou cinco réus.

De acordo com o relatório (PF, Ministério da Justiça Departamento de Polícia Federal, 2008), deu-se a investigação “uma vez que o banqueiro vinha intencionalmente criando obstáculos à concretização da venda da Brasil Telecom à Oi e essa postura estaria irritando membros do alto escalão do Governo Federal, interessados na concretização do negócio”.

É provável que a Polícia Federal teve o sigilo das informações desse caso quebrado pelo grupo hacker LulzSecBrasil, uma vez que o relatório citado está disponível no site do grupo hacker que encerrou suas atividades no Brasil. Outros casos iguais a esse, podem ser visualizados na Figura 1 .

Figura 1 - Print do site do grupo hacker com possível fraude a PF



Fonte: O autor.

O mundo está cada vez mais conectado, e os negócios empresariais são realizados via e-commerce, redes sociais, entre outros, a preocupação com os riscos que as empresas estão expostas, as vulnerabilidades e as ameaças que o mundo digital impõe são enormes. É enganoso acreditar que os alvos dessas fraudes são apenas os sites de governos. Em (Globo, Tecnologia e Games - Segurança Digital, 2011):

> Os ataques dirigidos – como são chamados os ataques e invasões realizadas de forma personalizada contra uma empresa – raramente recebem cobertura da imprensa. Isso porque muitos deles passam despercebidos.
>
> Mesmo assim, o ano de 2011 viu vários deles. Exemplos são a operação Dragão Noturno, contra empresas do ramo de petróleo, a invasão da empresa de segurança RSA – que por sua vez serviu para atacar a fabricante de armas Lockheed Martin -, ataques ao governo japonês e à também fabricante de armas Mitsubishi Heavy Industries e, finalmente, o vírus Duqu, que teria sido criado pelos mesmos programadores que fizeram o Stuxnex, um dos destaques de 2010 para atacar sistemas de controles industriais.

Ainda de acordo com Rohr em para o portal G1 da Globo (Globo, Tecnologia e Games, 2011):

> A bandeira do "antisec" levantada pelo Lulzsec está um tanto confusa, porque o movimento antissegurança não era destinado apenas a ataques contra o governo e corrupção, mas sim contra a indústria de segurança. Ao realizar os ataques que está realizando, os hackers estão – ao contrário do que prega o movimento – alimentando a indústria e a necessidade de profissionais.

Percebe-se a dimensão do problema quando profissionais que se dedicam a fornecer segurança para as empresas, (Globo, Tecnologia e Games, 2012) é "*Um dos acusados pelo governo norte-americano de fazer parte do grupo de hackers Lulz Security liderava uma organização sem fins lucrativos em Galway, na Irlanda, dedicada a manter sites mais seguros*". Em (UOL - IDG Now!, 2012) constata-se:

> Códigos eram de dois softwares corporativos, sendo que um não é mais fabricado; companhia de garante que dados de clientes estão protegidos.
>
> A fabricante de softwares de segurança Symantec confirmou que um grupo de hackers está em posse do código fonte de dois dos seus antivírus, sendo que um deles não é nem mais fabricado.
>
> "A Symantec pode confirmar que um segmento do seu código fonte usado em dois dos seus produtos corporativos mais antigos foi acessado, um dos quais já foi descontinuado. O código envolvido tem quatro ou cinco anos de existência", disse o gerente sênior da companhia para comunicações corporativas, Cris Paden.
>
> A confirmação acontece pouco depois de alegações recentes feitas por um grupo de hackers que copiou o código fonte do Norton Antivirus de servidores comprometidos que pertencem a agências de inteligência indianas.
>
> Paden confirmou que a falha de segurança não ocorreu na própria rede da Symantec, mas de uma entidade terceirizada. No entanto, ele se recusou a especular qual a identidade da rede até que a investigação em andamento revele mais informações.

Corrobora a premissa que não existe segurança absoluta, quando se constata que a indústria de segurança é alvo de grupos hackers e nem sempre está preparada com a segurança e proteção necessária.

2.1. Médias e Grandes Empresas

A segurança da informação em muitas empresas é gerenciada pela área de Tecnologia da Informação. Em outras onde a segurança da informação é fundamental e vital em todas as atividades da empresa, existe a tendência de que ela seja mantida pelo centro de gerenciamento de riscos.

Os processos de gerenciamento riscos visam elevar a qualidade da execução dos processos além de garantir o foco necessário para agregar valor ao negócio, maximizando o uso dos recursos próprios ou de terceiros, cada vez mais escasso, em proveito dos *stakeholders* da empresa.

Assim a atividade de gerenciamento de riscos é altamente estratégica em virtude da crescente complexidade dos serviços e produtos ofertados e da globalização dos negócios das empresas.

Os recursos financeiros e conhecimento técnico para a segurança da informação são dimensionados corretamente nas grandes e médias empresas, geralmente se apoiam na governança corporativa; na estrutura de gerenciamento e na metodologia de gerenciamento de riscos.

2.2. Governança Corporativa (GC)

Segundo o Código Brasileiro das Melhores Práticas de Governança Corporativa (IBGC, Instituto Brasileiro de Governança Corporativa, 2010) :

> Governança Corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, Conselho de Administração, Diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso a recursos e contribuindo para sua longevidade.

Para (Bertoldi, 2008) a governança corporativa tem como Princípios Fundamentais:

- **Transparência** (*disclosure*) – Está relacionado com a cultura de informar aos clientes, poderes públicos, acionistas, parceiros, financiadores, que vai além da obrigação de informar.
- **Equidade** (*fairness*) – É o tratamento equilibrado aos diferentes *stakeholders*, sem políticas discriminatórias, sem atitudes discricionárias.
- **Prestação de contas** (*accountability*) – Vai além do dever de prestar de contas da atuação dos agentes da governança corporativa, para quem os elegeu. Diz respeito às suas omissões e/ou reconhecimento dos erros, além da imputabilidade das decisões.
- **Responsabilidade corporativa** – sustentabilidade e responsabilidade social – Está diretamente relacionado com o sócio-ambiental numa perspectiva política, mais generalizada da estratégia empresarial, para com a sociedade/comunidade a qual a empresa está inserida, considerando todos os relacionamentos com a comunidade em seu habitat.

2.3. Planejamento Estratégico Corporativo (PEC)

A GC estimula a organização a desenvolver o PEC, que para (Castor, 2008) "*a Governança Corporativa e Planejamento Estratégico são, portanto, ferramentas complementares, para criar valor para os stakeholders e assim contribuir para a perenização da empresa*".

Assim, a ferramenta de gestão fundamental para as empresas, é o planejamento estratégico, para assegurar a sobrevivência no mercado, garantindo o desenvolvimento, além de direcionar o crescimento, definindo objetivos claros, estabelecendo diferenciais e garantindo vantagens competitivas para a organização, uma vez que define e padroniza a forma como a corporação deve comportar-se afim de atingir seus objetivos.

2.4. Governança da Tecnologia da Informação (GTI)

A GTI é parte da GC visto que a TI deve suportar e sustentar as estratégias e objetivos da corporação. É a GTI responsável por estabelecer o Planejamento Estratégico da Tecnologia da Informação (PETI) que obrigatoriamente deve estar alinhado ao PEC.

2.5. Planejamento Estratégico da Tecnologia da Informação (PETI)

O papel da TI nos processos de negócios das organizações possui relevância na gestão organizacional. O entendimento da importância acontece principalmente nas empresas que implementaram o PETI em conformidade com PEC, uma vez que essa conformidade promove ajustes contínuos no suporte que TI proporciona aos negócios, ao colocar em prática o que foi definido, contribuindo assim com a alta-administração nas tomadas de decisões estratégicas, isto é, no gerenciamento em alto nível.

O alinhamento dos planos dos *Chief Information Officers* (CIO) - gestores de tecnologia da informação - aos planos do *Chief Executive Officer* (CEO) - diretor geral – passa por colocar em prática as metas e objetivos desejados, e também por um acompanhamento e monitoramento contínuo, para promover ajustes sucessivos afim de manter o alinhamento da TI às estratégias do negócio.

2.6. Micro e Pequenas Empresas

Nas microempresas e empresas de pequeno porte, observa-se com alguma frequência, um gestor ou proprietário sem o mínimo conhecimento sobre gestão administrativa, pois a única coisa que conhece é o core business ou sua especialidade no nicho de mercado que ocupa.

O problema decorrente deste fato, é a existência de uma organização com pessoas que tomam decisões (para onde vão os recursos financeiros) e que ignora completamente o que significa a TI – Tecnologia da Informação para sua empresa, e qual o percentual de contribuição a TI representa no sucesso de seu negócio.

Se o conhecimento específico em administração já é parco, os investimentos a isso também o são, logo, é possível observar um comportamento idêntico na área de TI, mas numa proporção muito maior, culminando com um total descaso para a área de segurança da informação, levando em consideração investimento financeiro e conhecimento específico.

Quando muito, essas organizações investem em um profissional técnico de microinformática, que ocupa a função de Analista de Suporte, sem ter em seu staff um Administrador de Redes e muito menos um Administrador de Segurança, tudo isso evidentemente devido aos custos que isso acarretaria para a empresa.

Segundo (Carvalho, 2010, p. 13):

> De acordo o Anuário do Trabalho na Micro e Pequena Empresa (2010, online), as micro e pequenas empresas correspondem a mais de 90% dos 5,8 milhões de negócios formais existentes no Brasil e empregam mais de 50% dos trabalhadores com carteira assinada, o que corresponde a aproximadamente 13 milhões de empregados formalizados. A região sudeste é a que possui maior concentração de estabelecimentos formais, seguida pela região sul, nordeste, centro-oeste e norte, respectivamente.

De acordo com InformationWeek EUA em ITWEB as 100 mais inovadoras no Uso de TI, possuem métricas bem definidas, saber: a) As tecnologias utilizadas e o destino dos investimentos em Tecnologia; b) O grau de maturidade de gestão e governança de TI; c) O grau de maturidade dos processos de inovação e gestão do portfólio de projetos de TI; d) O papel da TI na empresa; e) Aplicabilidade versus custos; f) Gestão de recursos (benefícios versus riscos); g) Métricas de desempenho e; h) O grau de contribuição da TI para o negócio.

Nessa perspectiva, é possível afirmar que os fatores de medições aplicados são completamente ignorados no SOHO - Small Office e Home Office, ME - Micro Empresas e EPP - Empresas de Pequeno Porte, o que coloca em dúvida o futuro de 50% dos postos de trabalho formais.

Para que as empresas atinjam o sucesso em seus negócios, com a maximização da produtividade e competitividade, muitas fazem uso constantemente da tecnologia da informação. Daí decorre a necessidade em se ter um ambiente computacional confiável, garantindo assim um diferencial estratégico pelo essencial uso da informação em toda sua plenitude.

Para se alcançar um ambiente computacional confiável, é necessário garantir a segurança da informação bem como a sua disponibilidade; e isso é um desafio enorme para o mercado *small office home office* (SOHO), microempresa (ME) e empresa de pequeno porte (EPP) considerando que a segurança tende a ser proporcional ao investimento realizado.

A escolha da tecnologia de software deve levar em consideração a continuidade de negócio, sempre pensando em acompanhar o crescimento da empresa sem ter que alterar de forma abrupta a cultura e procedimentos relacionados à tecnologia porque a solução tecnológica atual não atende mais a demanda, ou porque o desenvolvedor não trabalha mais com aquele produto, ou ainda porque a empresa de desenvolvimento do produto faliu.

O mercado ME, EPP e SOHO não tem uma cultura empresarial amparada no continuísmo, esse mercado é conhecido pela falta de metodologia, falta de uniformização de processos ou padronização, falta de documentação, que não mensuram muito o custo de implantar uma versão ainda em desenvolvimento, ou uma versão pirata de alguma solução, tudo porque o custo é a tônica das decisões.

Há o entendimento que redução de custos pode ser alcançado pelo continuísmo de processos e manutenção de tecnologias existentes, e, que a busca por inovação e evolução com uma curva de aprendizagem não muito acentuada é aplicável não apenas para o hardware e o software de infraestrutura (Sistemas Operacionais, Suítes de Escritórios, Suítes de Segurança), mas também para sistemas de informação gerencial (ERP, CRM, BI, GED, CMS, KMS entre outros).

2.7. Endian UTM – Gestão Unificada Contra Ameaças

Tendo em vista que segurança depende radicalmente do nível de maturidade da empresa com seus processos de negócio e com seu gerenciamento de Tecnologia da Informação (TI), é preciso ter consciência que o firewall não é a única solução total e exclusiva de segurança, mas parte de um conjunto de sistemas de segurança aliado a procedimentos de pessoas conhecedoras das políticas de segurança da empresa e conscientes dos riscos advindos dos benefícios de estarem conectados ao mundo.

Observa-se na atualidade que algumas empresas souberam explorar o modelo de negócio do software open-source. Elas buscam disseminar o produto com uma versão comunitária para usuários domésticos, SOHO, ME e EPP. Com isso a empresa de desenvolvimento open-source tem uma ampla fatia de usuários que testam seus softwares, fazem sugestões, relatam bugs, etc.

Algumas melhorias são implantadas apenas em versões para serem comercializadas com dispositivos personalizados (appliances), casados com um contrato de manutenção com a garantia sobre o produto como um todo.

Esse tipo de empresa oferece um software voltado a uma empresa em fase de amadurecimento em sua cultura empresarial, que busca redução de custos, e que acima de tudo busca garantias de que a solução adotada proporcionará continuidade a seus negócios.

Essas ferramentas são desenvolvidas por empresas como Untangle e Endian, que usam o Linux e vários outros aplicativos de código aberto, no desenvolvimento de um gerenciamento de segurança unificado e centralizado, compostos de várias tecnologias focadas em segurança da informação.

O Endian UTM (Unified Threat Management) é uma família de produtos que busca evidenciar a usabilidade nas soluções específicas de proteção máxima contra roubo de dados, vírus, spyware, spam e outras ameaças da Internet, e por isso altamente especializada em segurança.

A empresa mantém um modelo de negócios comercializando os Endian Hardware Appliances, que são dispositivos de hardware com software para um determinado fim, do tipo "tudo em um". Não apenas o hardware como também o software comercializado, pode ter um contrato de suporte e manutenção.

A empresa mantém ainda a versão do Endian UTM Community disponível gratuitamente para download em seu site, além do código fonte do mesmo. Essa versão não tem suporte comercial, é, portanto, baseado no suporte de fóruns e comunidades específicas do produto.

Os recursos de segurança que ela proporciona para a empresa usuária, são: Firewall, DMZ – Zona Desmilitarizada, Proxies, NAT - Network Address Translation, VPN – Virtual Private Network com OpenVPN e IPSec, Autenticação/Certificação, IPS - Intrusion Prevention System, DHCP - Dynamic Host Configuration Protocol, NTP - Network Time Protocol, Controle de tráfego, Supervisor de Conteúdo, Antivírus.

---

3. Considerações Finais

Abordagem qualitativa muitas vezes mostra-se adequada à compreensão dos aspectos inseguros da vida humana em grupos empresariais no uso da tecnologia de informação. Com isso, um enfoque interpretativo da realidade em um campo natural (empresas) mostra-se

apropriado.

Observa-se assim uma lacuna a ser preenchida com iniciativas de trabalhos acadêmicos, e principalmente com terminativas práticas que proporcionem aumento expressivo na segurança da informação nestes cenários.

Ao se propor uma solução tecnológica, para estudo prático no ambiente empresarial, não se pode esquecer do cunho Business que toda solução deve ter, haja vista os vários frameworks que surgiram de melhoras práticas de TI, justamente para alinhar a TI as necessidades do negócio como um todo, cito: ITIL, COBIT, etc.

Propor o uso de uma plataforma de segurança de fácil implantação e manutenção, necessitando pouco investimento e CTP - Custo Total de Propriedade reduzido, de rápida recuperação de desastres, tem um apelo principalmente para redes pequenas.

Tal plataforma deve ser sugerida, desde que ela simplifique o desenvolvimento de soluções de segurança, ao mesmo tempo em que as tornam capazes de fornecer recursos só encontrados em soluções de alto custo financeiro, bem como de um vasto conhecimento técnico.

Assim, a eficiência e custos adequados evidenciam quando se propõe uma solução que tenha uma menor complexidade de software e componentes de hardware, aliado ao fato de não exigir uma extensa capacitação dos profissionais envolvidos nos processos de segurança da informação.

Em alguns casos é possível propor apenas o software em sua versão comunitária com custos tendendo a zero. Porém, o fato da aplicação ter custo zero não deixa de ter relevância na abordagem que visa a continuidade e curva de aprendizagem suave. O custo zero não deve ser a tônica principal.

Deve-se buscar formas de agregar mais segurança à esses pequenos empresários, sem a necessidade de grandes investimentos financeiros e tampouco demandando na contratação de um profissional altamente especializado para manter o serviço.

De modo que, com essas facilidades amplamente difundidas, contribuirão para a minimização de riscos, não apenas à pequena empresa, mas também para a grande rede mundial (Internet), uma vez que possível ser multiplicadores de insegurança caso não a considere como importante.

Referências bibliográficas

Gobo, Dossiê Globo News. (2014). “Tentei matar Saddam, só lamento não ter conseguido”, diz ex-agente - GloboNews - Vídeos do programa Dossiê GloboNews - Catálogo de Vídeos. Recuperado 6 de outubro de 2016, de http://g1.globo.com/globo-news/dossie-globo-news/videos/v/tentei-matar-saddam-so-lamento-nao-ter-conseguido-diz-ex-agente/1620911/

Globo, Tecnologia e Games. (2012, setembro 3). Hacker acusado de ser do LulzSec trabalhava com segurança na Irlanda. Recuperado 7 de outubro de 2016, de http://g1.globo.com/tecnologia/noticia/2012/03/hacker-acusado-de-ser-do-lulzsec-trabalhava-com-seguranca-na-irlanda.html

UOL - IDG Now! (2012, junho 1). Symantec confirma roubo de código fonte de antivírus. Recuperado 7 de outubro de 2016, de http://idgnow.com.br/seguranca/2012/01/06/symantec-confirma-roubo-de-codigo-fonte-de-antivirus/

Jornal do Brasil. (2012, maio 4). Monte Carlo: agente da Abin envolvido em esquema de Carlinhos Cachoeira. Recuperado 6 de outubro de 2016, de http://www.jb.com.br/pais/noticias/2012/04/05/monte-carlo-agente-da-abin-envolvido-em-esquema-de-carlinhos-cachoeira/

Jornal O Estado de São Paulo. (2012, Fevereiro). Justiça Federal absolve Dantas no caso Kroll - Política. Recuperado 6 de outubro de 2016, de http://politica.estadao.com.br/noticias/eleicoes,justica-federal-absolve-dantas-no-caso-kroll-

imp-,835560

Globo, Tecnologia e Games - Segurança Digital. (2011, dezembro 19). Retrospectiva 2011: LulzSec, vazamentos e vírus de Mac. Recuperado 7 de outubro de 2016, de http://g1.globo.com/tecnologia/blog/seguranca-digital/post/retrospectiva-2011-anti-sec-lulzsec-invasoes-e-virus-de-android.html

Globo, Tecnologia e Games. (2011, junho 27). Caos, intrigas e discordância marcam Lulzsec do Brasil. Recuperado 7 de outubro de 2016, de http://g1.globo.com/tecnologia/noticia/2011/06/caos-intrigas-e-discordancia-marcam-lulzsec-do-brasil.html

Jornal do Brasil. (2011, junho 24). Hackers do LulzSec indicam ataque ao site da Globo.com. Recuperado 7 de outubro de 2016, de http://www.jb.com.br/pais/noticias/2011/06/24/hackers-do-lulzsec-indicam-ataque-ao-site-da-globocom/

Carvalho, S. A. de. (2010, novembro 22). *Características identitárias brasileiras: suas influências na pequena empresa* (Dissertação). Universidade de São Paulo. Recuperado de http://www.teses.usp.br/teses/disponiveis/27/27154/tde-17022011-123551/

IBGC, Instituto Brasileiro de Governança Corporativa. (2010). Código Brasileiro das Melhores Práticas de Governança Corporativa. Instituto Brasileiro de Governança Corporativa. Recuperado de http://www.ibgc.org.br/userfiles/Codigo_julho_2010_a4.pdf

LASEC/EPFL, S. and C. L. (2009). Compromising Electromagnetic Emanations of Wired and Wireless Keyboards - Martin Vuagnoux and Sylvain Pasini. Recuperado 6 de outubro de 2016, de http://lasecwww.epfl.ch/keyboard/

Castor, B. V. J. (2008, novembro). *Planejamento Estratégico*. CASTRO.pdf. Recuperado de http://www.ibgc.org.br/Download.aspx?Ref=Eventos&CodArquivo=169

Bertoldi, M. M. (2008, junho). *Governança Corporativa e a 3a reforma da Lei das S/A*. BERTOLDI,M_Jun2008_Lei.pdf. Recuperado de http://www.ibgc.org.br/Download.aspx?Ref=Eventos&CodArquivo=133

PF, Ministério da Justiça Departamento de Polícia Federal. (2008). Análise de Dados: O Caso Opportunity-Brasil Telecom. Recuperado de lulzsecbrazil.org/policia-federal/01/Export/4674.doc

Rogerio, F. C. (2007). *Planejamento Estratégico Tecnologia da Informação Orientado ao Alinhamento Negócios das Empresas - Caso do grupo CIO's Santa Catarina* (Dissertação). Universidade do Estado de Santa Catarina, Florianópolis - SC. Recuperado de Francisco.pdf.

---

1. M.Sc., Universidade Federal Fluminense – UFF – (manassesvicente@id.uff.br)

Revista ESPACIOS. ISSN 0798 1015
Vol. 38 (Nº 19) Año 2017

[Índice]