AMEAÇAS INTERNAS – DESAFIOS DA SEGURANÇA E IMPACTOS CAUSADOS POR COLABORADORES NO AMBIENTE DE TI

INTERNAL THREATS - SECURITY CHALLENGES AND IMPACTS CAUSED BY EMPLOYEES IN IT ENVIRONMENT

ARAÚJO, Aline Lima [1]

ARAÚJO, Régis de Oliveira [2]

email: allynelimaa@gmail.com[1], rgs.araujo@hotmail.com[2]

Resumo:

Este artigo aborda os diversos desafios na implantação e gestão de Segurança da Informação, não apenas em instituições de pesquisa, mas também em corporações. A pesquisa foca nos nos riscos causados pela má utilização dos recursos de rede que tendem a causar incidentes como perda de dados e vazamento de informações. Uma das soluções identificadas se apresenta na educação e treinamento dos usuários da rede e também da correta aplicação de políticas que regulem o uso de ativos de Tecnologia da Informação.

Palavras-chave: integridade; disponibilidade; confidencialidade; segurança; ti.

Abstract

This paper addresses the different challenges found when deploying and managing Information Security, not just on research institutions, but also in corporations. The research focuses the risks caused by the misuse of network resources that, in the future tends to cause incidents such as data loss and information leakage, which one of the addressed solutions is defined on network users' education and training and also the correct implementation of policies that regulate the Information Technology assets utilization.

Keywords: integrity; availability; confidentiality; security; it.

1 INTRODUÇÃO

Com o crescimento significativo do número de ameaças na Internet, o número de riscos nas redes corporativas têm exigido uma maior atenção dos gestores de segurança da informação. De acordo com o relatório sobre ameaças à segurança na internet [Symantec 2012b] elaborado pela Symantec, o Brasil assumiu em 2011 a 4a posição no ranking mundial de propagadores de atividades maliciosas.

Baseado no cenário atual de Segurança da Informação no ambiente corporativo, este artigo aborda os desafios que podem ser encontrados para manter o compliance (regularidade com as políticas internas) nas organizações, tendo como foco principal a importância da colaboração do usuário final e a aplicação correta das políticas de segurança nas corporações.

O objetivo é alertar que corporações detentoras de uma política de segurança rígida e colaboradores cientes dos riscos a que estão expostos diariamente, garantam com mais facilidade a integridade da rede e de seus dados. Para tanto, foi utilizado como base o estudo de caso sobre a gestão de TI (Tecnologia da Informação) na Fundação Oswaldo Cruz (conhecida como Fiocruz) realizado por Paulo Eduardo Potyguara Coutinho Marques [Marques 2011].

Este artigo evidencia as necessidades que toda organização possui de orientar seus profissionais colaboradores no que tange à Segurança da Informação. As empresas que investem fortemente em segurança da informação conseguem economizar US$ 1,6 milhão por ano [HP/Ponemon 2012a]. Trata também de aprofundar a observação e estudo dos desafios encontrados por profissionais dessa área, bem como das diversas ferramentas e técnicas criadas para que a gestão e manutenção do compliance se façam possíveis.

O Caso da Fiocruz é brevemente descrito na seção 2, seguido das ameaças de segurança na seção 3, onde são abordadas e exemplificadas as fontes que causam os riscos na segurança. A importância da implantação e uso correto das políticas de segurança, bem como a educação do usuário são explanadas nas seções 4 e 5, seguidas dos incidentes de segurança e os riscos que as novas tecnologias podem trazer para o mundo corporativo, descritos nas seções 6 e 7.

As seções 8 e 9 abordam a importância da utilização correta das ferramentas de TI e como a Segurança da Informação pode beneficiar o mundo corporativo. A conclusão do artigo é marcada pelo desfecho do assunto bem como pelas considerações finais que envolvem o tema tratado.

2. A PESQUISA NA FIOCRUZ

Apresentada em abril de 2011 por Paulo Eduardo Potyguara Coutinho Marques, a dissertação de mestrado intitulada “Tecnologia da Informação na Fundação Oswaldo Cruz” se desenvolveu através da apresentação de dados coletados em pesquisa de natureza exploratória realizada pelo próprio autor.

A Fundação Oswaldo Cruz é uma Instituição Pública vinculada ao Ministério da Saúde com a missão de produzir, disseminar e compartilhar conhecimento e tecnologias voltadas para o fortalecimento e a consolidação do Sistema Único de Saúde (SUS) [Portal Fiocruz 2012].

A referida pesquisa tratou de diagnosticar a situação da TI na fundação com destaque para os diversos problemas encontrados e o modelo falho de gestão de TI.

Dentre os problemas encontrados pelo pesquisador observam-se aqueles relativos ao padrão de Segurança da Informação na instituição, que provou não dispor de documentação e nem de um modelo de gerenciamento centralizado e uniforme entre as diversas unidades da fundação.

É com base no fato de que as diretrizes de Segurança da Informação (Confidencialidade, Integridade e Disponibilidade) não foram encontradas na instituição que o presente artigo se desenvolve, explanando o padrão encontrado na Fiocruz ao passo que apresenta as políticas e diretrizes para o modelo de gestão de Segurança da Informação ideal [Watkins 2008].

A seguir são discutidos os diferentes vetores de ameaças e o impacto que os mesmos causam na produtividade e negócio das companhias.

3. FONTES DE AMEAÇAS

Independente do tamanho da empresa, do seu ramo de negócios, do número de colaboradores e do quão bem estruturado é seu modelo de gestão de Segurança da Informação, se existe uma rede de computadores implementada sempre existem ameaças digitais vindas de todas as origens (ataques de fora da empresa ou vulnerabilidades exploradas por pessoas com acesso autorizado aos sistemas) tentando penetrar as barreiras montadas.

Os pontos acima citados, como por exemplo, o ramo de negócios, são questões relevantes quando se considera o nível de instrução tecnológica e conhecimento dos riscos que cada usuário pode trazer para a rede da companhia, mas, independentemente disso, é inevitável que dado certo espaço de tempo alguma ameaça tente se instalar nessa rede e causar danos.

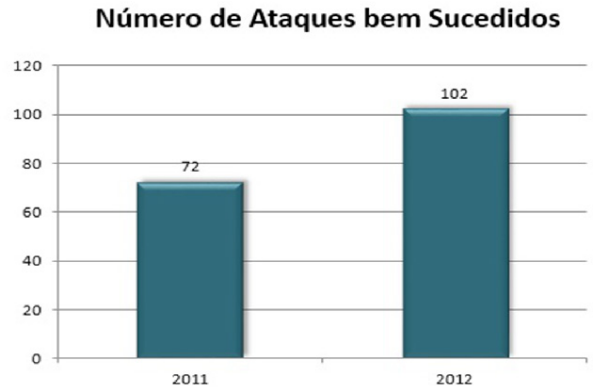
Até mesmo uma instituição de renome como a Fundação Oswaldo Cruz está sujeita a essas ameaças. No mencionado estudo de caso - feito na instituição, é diagnosticada a necessidade de reconstruir toda a estrutura de TI da Fundação, em especial no que tange às diretrizes de Segurança da Informação (Confidencialidade, Integridade e Disponibilidade):

> "[...] TI na Administração Pública Federal carece de planejamento estratégico institucional, possui deficiência na estrutura de pessoal e trata de forma inadequada as informações, ferindo a confidencialidade, integridade e disponibilidade das mesmas. [...]

Os três pilares da segurança da informação (confidencialidade, integridade e disponibilidade), são o escopo da Segurança da Informação definido pela ISO 27001.

Para que seja possível alcançá-los é essencial saber as diversas fontes conhecidas de ameaças, bem como estar ciente de que novas podem surgir a qualquer momento.

Figura 1: Número de Ataques bem Sucedidos - HP/ Ponemon



Seguem alguns exemplos das diferentes fontes de ameaças existentes:

- Vírus baixados de sites da Internet ou levados por meio de dispositivos móveis para a empresa – são algumas das fontes mais comuns de geração de incidentes de segurança (evento que infringe a política da empresa e necessita de ação para correção – é discutido com detalhes posteriormente).
- Vazamento de Informações (Information Leakage) seja ele intencional ou não: responsável inclusive pela perda de concorrências e patentes de mercado. Trata-se da divulgação para uma ou mais pessoas (físicas ou jurídicas) de informações consideradas confidenciais. Podem ocorrer de diversas formas, como por exemplo um usuário que possui acesso a determinado documento confidencial faz o download do mesmo para seu smartphone. Esse aparelho é então roubado. Caracteriza um incidente de segurança por vazamento de informações confidenciais. Em 2006, um laptop de um analista de dados foi roubado. Ele continha dados pessoais e de saúde de cerca de 26,5 milhões de soldados americanos ativos e veteranos [Government Executive 2006].

Outros exemplos de responsáveis por vazamento de informação são vírus de computador desenvolvidos para captura de informações (como o Infostealer [Symantec 1997]) que podem fazer cópias de documentos confidenciais. Da mesma forma, senhas fracas para logon na rede são facilmente descobertas por indivíduos mal intencionados (através de técnicas de força bruta ou de engenharia social) que podem utilizá-las para obtenção de informações confidenciais sobre a empresa.

Um usuário deixar documentos confidenciais sobre a mesa e sair de seu posto de trabalho, por exemplo, para beber água, pode ser considerado um incidente de segurança, pois, certo visitante mal intencionado (colaborador da empresa ou não) pode tirar proveito dessa situação e fazer uma cópia desse documento. Esse tipo de incidente é descrito na chamada Política da Mesa Limpa da ISO 270001.

De forma semelhante, um usuário que deixa sua estação e não bloqueia sua área de trabalho também é responsável pela geração de um incidente de segurança. As credenciais disponíveis em sua estação desbloqueada podem ser suficientes para que alguém faça, por exemplo, uma cópia de algum

documento restrito.

• Apesar de muitos usuários não aprovarem, uma política que proíbe o download de anexos de e-mail pode ser bastante eficaz no estabelecimento da Segurança da rede.

Usuários com pouco conhecimento técnico tendem a acreditar em mensagens de e-mails externos cujas fontes nem mesmo são conhecidas, representando também nesse caso, um incidente de segurança.

Existem diversas ações que podem ser tomadas por administradores de rede para evitar impactos causados pelas diferentes fontes de ameaças existentes.

Como está explanado a seguir, as políticas de Segurança da Informação definem a base para o fluxo e manipulação segura dos dados de uma companhia, representando papel crucial na gestão da Segurança.

4 POLÍTICAS DE SEGURANÇA

Ao implementar uma rede de computadores é de suma importância que haja um planejamento eficaz das políticas de Segurança da Informação onde devem ser previstos todos os pontos fracos que escolhas diversas podem vir a gerar na rede.

Esse planejamento deve possuir como resultado um documento comumente chamado de "Política de Segurança da Informação" e deve ser de conhecimento de todos os colaboradores que acessam a rede da empresa.

Algumas companhias costumam promover treinamentos periódicos para garantir que a ampla divulgação da política seja estabelecida.

Essas e outras atitudes geram um custo considerável na receita de qualquer companhia, mas é comprovado que a economia que o investimento em Segurança da Informação gera é consideravelmente maior. O custo anual causado por ataques a empresas dos Estados Unidos é de US$ 8,9 milhões [HP/ Ponemon 2012b].

As políticas de Segurança da Informação buscam também uniformizar o pensamento dos colaboradores com relação à percepção e o cuidado com a rede e as informações que nela trafegam.

Na Fiocruz foi evidenciada uma disparidade nos processos de TI conhecidos pelos profissionais da área. Disparidade essa que é transmitida para o âmbito da Segurança da Informação na instituição:

> "[...]Percebe-se aqui que a fragmentação da área de TI e o desconhecimento da mesma no âmbito da Fiocruz tornam mais que evidente a necessidade de uma política de TI para a instituição e o seu papel no planejamento da mesma. [...]

A Administração Pública Federal ao conhecer a falha na gestão de TI da Fiocruz passou a utilizar o SISP (sistema instituído com o objetivo de gerir os recursos de informação e informática da Administração Pública Federal Direta, Autárquica e Fundacional) como modelo a ser seguido na administração de Tecnologia da Informação na instituição:

> "[...]O SISP tem por finalidade, garantir que os pilares da Segurança da Informação (confidencialidade, integridade e disponibilidade), sejam atendidos em sua plenitude na Administração Pública Federal. [...]

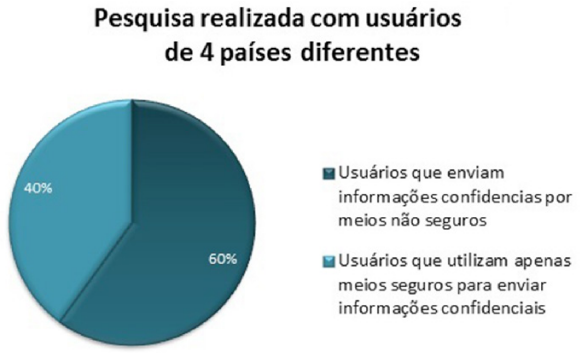
4.1 Restrições de Acesso à Internet

O uso irrestrito da Internet em ambiente corporativo causa a perda de produtividade entre os colaboradores e o desperdício de recursos computacionais (como banda de internet, por exemplo). Em pesquisa realizada em 2008, 87% dos trabalhadores brasileiros que utilizavam computadores pessoais (PC, na sigla em ingês) faziam uso da internet em horário de trabalho [Instituto Qualibest 2008], mas a perda da produtividade não é o maior problema causado pela navegação na Web de forma indiscriminada.

A Internet é hoje uma importante ferramenta de trabalho para toda empresa, integrando o fluxo de comunicação, conexão com clientes, fornecedores e o mundo externo de forma geral. É justamente esse grande poder que a internet proporciona que necessita ser controlado. Usuários comuns da rede, em sua maioria, não sabem dos riscos que expõem a si próprios e à companhia na qual trabalham ao navegar na Web.

A Figura 2 apresenta os resultados de pesquisa realizada com usuários de quatro países diferentes [Trend Micro 2010] e mostra que a maioria dos usuários assume que envia informações confidenciais das empresas sem se preocupar com a segurança:

Figura 2: Utilização de meios seguros para envio de informações confidenciais - Trend Micro



Existem muitas ferramentas do tipo Proxy (servidor que concentra a saída de internet e permite manipulação de regras de bloqueio baseadas em políticas predefinidas) que oferecem recursos à equipe de Segurança da Informação para o controle dos acessos à internet. Porém, essas ferramentas servem apenas como auxiliares para tal tarefa, uma vez que o alicerce do gerenciamento da internet deve ser embasado na Política de Segurança da Informação da referida empresa.

4.2 Controle de Acesso Lógico

Outra preocupação em nível de moderação de acesso presente no backlog (lista de pendências) dos administradores de rede e segurança é o controle do acesso lógico [Stamp 2006]. Atividade que requer um grande e complexo mapeamento dos diversos perfis de utilizadores presentes na rede.

Com o controle de acesso é possível delegar permissões específicas àqueles que as necessitam, bem como negar permissão a diretórios e execução de determinadas tarefas que, segundo mapeamento,

não são de responsabilidade de qualquer usuário.

Os problemas que podem ser causados por falha (ou até mesmo ausência) do mapeamento desses perfis são diversos. Por exemplo: usuários desastrados podem apagar um diretório raiz que contém dados importantes de toda a companhia ou, um vírus de computador como o W32.Stikpid [Symantec 2012c] é instalado num servidor de arquivos (fileserver) com permissões abertas, onde o vírus do tipo worm tem a capacidade de esconder as pastas do servidor de arquivos caso o usuário de sistema utilizado pelo mesmo (geralmente usuário final da rede) esteja com as permissões para tal alteração.

4.3 Política de Mesa Limpa

A Segurança da Informação não está apenas ligada aos ativos de informática da empresa, mas sim de toda a informação gerada ou manipulada pelos colaboradores da companhia [ISO 2005]. A Política da Mesa Limpa estabelece regras para a correta manipulação de documentos não digitais nas mesas de trabalho.

É importante que a política seja adequada ao negócio da empresa bem como ao ambiente de trabalho de cada divisão ou departamento da companhia.

Seguem alguns exemplos de quebra da política de Mesa Limpa que comumente geram incidentes de segurança:

- Gaveta destrancada – esta pode possuir documentos pessoais ou da empresa, considerados confidenciais.
- Agenda sobre a mesa – Esta pode conter informações pessoais e profissionais como números de telefone, senhas, topologias, etc.
- Telefone celular ou crachá da empresa sobre a mesa. Celulares contêm números de telefones de clientes e fornecedores. O crachá da empresa muitas vezes é utilizado para prover acesso físico a diferentes setores da empresa.
- Senha anotada no post-it colado em objetos na mesa: pode permitir acessos maliciosos (intrusão).

A política de mesa limpa e as demais políticas da Segurança da Informação são itens que precisam ser apresentados periodicamente aos usuários da rede a fim de desenvolver a educação dos usuários com relação ao uso consciente dos ativos de TI, como é mostrado à seguir.

5 EDUCAÇÃO DO USUÁRIO

Mais importante do que os administradores da rede terem conhecimento dos riscos que o ambiente de TI corre é a conscientização dos usuários que utilizam os sistemas computacionais.

Como citado anteriormente, grandes empresas comumente realizam treinamentos periódicos sobre Segurança da Informação com o objetivo de disseminar entre os colaboradores as normas e diretivas registradas na Política de

Segurança da Informação. Porém, apresentar a política de segurança nem sempre é suficiente para o estabelecimento de uma rede segura.

É preciso educar os usuários acerca das práticas de utilização dos ativos de TI. Muitos usuários utilizam o computador da empresa com a mesma negligência que o fazem com seu computador pessoal, em ambiente domiciliar.

Esses e outros vícios no padrão de utilização de dispositivos podem comprometer dados confidenciais da empresa e precisam ser compreendidos e combatidos pelo departamento de Segurança da Informação.

Na Fundação Oswaldo Cruz, foi mapeado um déficit no conhecimento daqueles que utilizam a tecnologia da instituição:

> "[...]o simples uso da tecnologia da informação ou de outro tipo de tecnologia não terá impacto positivo sobre o desempenho organizacional, incluindo a lucratividade e a qualidade dos processos e produtos, se não houver um investimento considerável na capacitação dos recursos humanos.[...]"

Esse é um processo constante e interminável (afinal, novos colaboradores são contratados a todo tempo) e que requer reformas periódicas a fim de adequar a norma às mudanças ocorridas no cenário corporativo no âmbito da Segurança da Informação. 370 000 tablets foram vendidos no Brasil no primeiro trimestre de 2012. Destes, 12% foram destinados ao mercado corporativo e de governo [IDC Brasil 2012b]. É de suma importância que a política seja revisada e os usuários conscientizados do impacto que seus novos dispositivos podem trazer ao negócio da empresa, a fim de que o novo padrão seja compreendido e, também, de que os novos riscos sejam mitigados.

O comportamento inadequado dos usuários da rede gera os chamados Incidentes de Segurança. Esses por sua vez, são explanados na seção à seguir.

6 INCIDENTES DE SEGURANÇA

Qualquer evento adverso, que possa ameaçar os pilares de segurança (Confidencialidade, Integridade e Disponibilidade)- é considerado um Incidente de Segurança [Microsoft Technet 2012]. Esses incidentes são os responsáveis por falhas na segurança e devem ser prevenidos e tratados antes que se tornem um problema. Alguns exemplos de eventos são a violação da política interna de segurança e infecções adquiridas na web ou através de dispositivos móveis.

Muitas vezes não é possível evitar um incidente, quando isso acontece é de extrema importância que haja uma resposta para o mesmo. Através de estratégias de gestão de riscos de segurança e a prática constante de resposta a incidentes é possível minimizar o impacto na rede [Dantas 2006].

A equipe responsável deve ter definido um plano de respostas a incidentes e seguir seriamente as diretivas de gerenciamento. Além disso, é preciso documentar todas as fases do plano e discutir internamente os aspectos que podem ser melhorados. Atividades como monitoração do

tráfego de rede, avaliação dos logs (históricos de atividades) e vulnerabilidades do ambiente, monitoramento dos processos de backup e restauração, atualização dos sistemas, servidores e estações devem ser realizadas frequentemente pela equipe [Microsoft 2012a].

Além de beneficiar a integridade da rede, a política de resposta a incidentes também pode beneficiar financeiramente as corporações, pois quando o ataque é evitado não há prejuízo e, consequentemente, os gastos com recuperação dos dados são economizados.

Um incidente de segurança pode surgir a qualquer momento e em qualquer lugar e a utilização de novas tecnologias pode facilitar sua ocorrência com mais frequência na rede. Esse assunto é abordado com detalhes na próxima seção.

7. NOVAS TECNOLOGIAS DE TI E OS RISCOS À SEGURANÇA QUE ELAS REPRESENTAM

O aumento da utilização de novas tecnologias também é responsável pela maior ocorrência de incidentes de segurança. A busca pela acessibilidade e economia de tempo torna as empresas cada vez mais reféns das novas tecnologias. O grande problema é que nem sempre as corporações estão atualizadas e preparadas o suficiente para manter a proteção de sua rede e tornam-se vulneráveis às ameaças que surgem a todo o momento.

As ameaças de segurança também são encontradas nos dispositivos móveis como smartphones, tablets e notebooks. O gráfico apresentado na figura 3 mostra a percepção de representantes de algumas empresas do Brasil com relação à computação móvel.

Figura 3: Nível de risco com a mobilidade na visão das empresas - [Symantec 2012a]

É possível notar na Figura 3 que diante da questão "Como você caracterizaria o nível de risco que sua organização enfrenta com a computação móvel?", muitos acreditam que os riscos sejam neutros ou baixos. Isso pode ser um grande problema para Segurança da Informação, pois os dispositivos móveis podem ser os causadores de incidentes de segurança.

O uso desses dispositivos no dia-a-dia empresarial teve crescimento significativo nos últimos tempos [Symantec 2012a]. A Pesquisa sobre a Situação da Mobilidade, realizada pela Symantec no Brasil entre agosto e novembro de 2011, também mostra que a computação móvel proporcionou crescimento em relação à eficiência dos negócios.

De fato esses dispositivos tornaram-se uma ferramenta de trabalho cada vez mais essencial e indispensável para os negócios- 42% das empresas no Brasil possuem funcionários que utilizam seus próprios dispositivos móveis para acessar

informações corporativas (Bring Your Own Device, BYOD) [IDC Brasil 2012a].

A área de Tecnologia enfrenta dificuldades no gerenciamento da segurança do controle da utilização dos dispositivos móveis (Relatório sobre Segurança da Informação nas Empresas – [Symantec 2011]), por isso, esse é um dos grandes desafios para a equipe de segurança da informação. É preciso ter políticas definidas e estar ciente dos riscos a que a rede é exposta ao permitir o uso desses dispositivos.

O usuário pode infectar a rede com seu dispositivo móvel, por isso a política de educação do usuário tem suma importância. É preciso que todos tenham ciência dos riscos a que estão expostos e dos prejuízos que podem causar à corporação. Além disso, sempre há alguém tentando infectar a rede de alguma forma, por isso o uso correto das ferramentas de segurança pelos profissionais de TI também é extremamente relevante.

8. FERRAMENTAS DE SEGURANÇA

Além das políticas de segurança e cuidados com os usuários, outros recursos devem ser utilizados para manter a rede segura:

- Antivírus: É um software que detecta e neutraliza o vírus, protegendo o computador contra ataques de softwares mal intencionados [Microsoft 2012b]. Ao configurar o antivírus é possível definir a lista de exclusão, onde são listados os arquivos, caminhos ou extensões a serem liberados, no entanto, ao configurar uma lista de exclusão é preciso ter ciência dos riscos a que a rede ficará exposta.
- Antispam: Ferramenta responsável pela proteção contra Spams que são mensagens de anúncios ou envio de links ou softwares maliciosos, com o intuito de promover produtos ou serviços podendo induzir usuários a cair em fraudes ou causar danos à rede de destino.
- Antispyware: Ferramenta responsável pela proteção contra ataques de Spywares (programas que transmitem informações pessoais sem o consentimento do usuário). Milhares de pessoas são vítimas de Spywares diariamente e em muitos casos esses softwares são instalados de forma legal pelo próprio usuário que executa a instalação muitas vezes sem perceber [McAfee 2005].
- Antiphishing: Previne contra ataques de Phishings que são os responsáveis por tentar obter informações daquele que os recebem. Phishing comumente utiliza-se de engenharia social para obter informações pessoais, tais como: usuário, senha, endereço, etc.
- Firewall: Realiza a proteção com base em uma política de segurança (definida pela empresa), funciona como uma barreira responsável por controlar o fluxo de entrada e saída de informações na rede. Existem Firewalls em forma de hardware e software [Kurose 2010].
- IPS (Intrusion Prevention System): Ferramenta utilizada para bloqueio de ataques baseado em assinaturas pré-existentes. É capaz

de detectar atividades maliciosas externas e de usuários. É normalmente utilizado para garantir que os dados que passaram pelo Firewall não se tratem de pacotes maliciosos ou corrompidos.

A implementação correta desses recursos auxilia na segurança da rede, para isso é preciso manter essas ferramentas de segurança atualizadas. Este procedimento deve fazer parte da estratégia de gestão de riscos da corporação, pois é essencial para garantir a segurança.

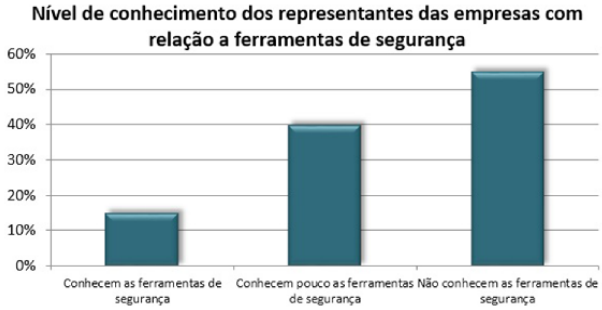
Um exemplo real é a falha na gestão de TI da Fiocruz, a falta de atualização de softwares dificultou a funcionalidade correta e a integridade e segurança da rede:

> "[...]Na questão da estrutura de microinformática, a Fiocruz encontra-se defasada em relação à tecnologia existente. [...]cerca de 77% das estações de trabalho utilizam o sistema operacional Windows XP, entretanto a Microsoft, detentora do direito de copyright deste, publicou que o suporte mainstream a este sistema operacional terminou em 14 de abril de 2009. {Microsoft Corporation, 2011}.{...}

Ataques surgem a todo momento, é preciso estar atualizado em relação aos softwares e outras tecnologias instaladas na empresa. Geralmente, as empresas desenvolvedoras disponibilizam frequentemente atualizações de suas ferramentas, nesse caso, cabe aos profissionais responsáveis manter seus sistemas e equipamentos atualizados.

A Figura 4 sintetiza uma pesquisa realizada com 206 empresas no Brasil onde é revelado que a maioria não sabe quais ferramentas de seguranças devem ser adquiridas [IDC Brasil 2012a]:

Figura 4: Nível de Conhecimento das Ferramentas de Segurança - IDC Brasil



Este também pode ser um problema para a segurança, as corporações devem estar cientes de que é preciso investir tanto em recursos para área de TI quanto em profissionais qualificados capazes de identificar as necessidades e as melhores soluções para empresa.

Os recursos devem ser disponibilizados para manter a área de tecnologia atualizada, as corporações devem estar cientes de que é preciso investir. A área de TI deve ser tratada como aliada, dessa forma muitos benefícios podem ser adquiridos.

9. BENEFÍCIOS PARA A EMPRESA

A tecnologia da informação torna-se cada vez mais necessária para a integridade das informações de qualquer empresa.

No entanto, é importante trabalhar com a tecnologia de forma que ela seja aliada e não inimiga do negócio.

A pesquisa realizada na Fiocruz também mostra de forma clara a importância da TI:

> "[...]A partir desta pesquisa e da análise realizada, é possível concluir que o alinhamento estratégico da Tecnologia da Informação tem o poder de potencializar a atuação da Fiocruz no Sistema Único de Saúde. [...]

Ou seja, o investimento na busca de novas soluções tecnológicas também é essencial, mas, além disso, a empresa deve investir nas políticas de educação do usuário. Conforme citado nas seções anteriores, diversos problemas na segurança são causados pelos usuários (intencionalmente ou não).

Quando não aplicada de forma segura por todos, a tecnologia da informação pode ser um grande inimigo dos negócios e da empresa. Informações confidenciais podem ficar expostas ou serem acessadas facilmente por desconhecidos, o que pode facilitar um ataque, gerando assim prejuízos para empresa.

Contudo, é possível notar ao longo do artigo que a segurança da informação é a ferramenta necessária para garantir que o TI traga benefícios às empresas. Com a rede segura é possível utilizar todas as ferramentas e recursos que a tecnologia disponibiliza a favor do negócio.

Sabe-se que nos dias atuais a agilidade nas decisões e obtenção de informação é uma das principais ferramentas para garantir o sucesso de qualquer corporação. As ferramentas disponibilizadas pelo avanço tecnológico tornam mais simples os trabalhos dos funcionários e garantem soluções mais ágeis e assertivas, independente da área de atuação.

10. CONCLUSÃO

A quantidade e a magnitude dos desafios que administradores de redes e segurança encontram em seu dia-a-dia têm crescido exponencialmente nos últimos anos com o advento de novas tecnologias. No entanto, lidar com novidades não é o único problema que os profissionais dessa área precisam enfrentar. Os colaboradores da própria companhia tendem a se tornar (na maioria dos casos) os principais vetores de quebras de segurança.

Este artigo trata de explanar a importância do investimento na educação dos usuários, no que diz respeito à Segurança da Informação, bem como de descrever os conceitos envolvidos na definição de uma política de Segurança que serve como base para a conscientização daqueles que fazem uso do ambiente de TI. A importância de uma política bem definida é exemplificada com estudo de caso realizado na Fundação Oswaldo Cruz, citada ao longo do artigo e que mostrou diversas deficiências na gestão de TI, com destaque àquelas relacionadas à Segurança da Informação.

Conforme citado no artigo, é possível identificar uma ausência considerável de documentação, procedimentos e processos que auxiliem na administração da segurança na instituição e que causam um desalinhamento entre os profissionais de TI da entidade nas diversas unidades da Fiocruz. Foi identificada a necessidade da realização de treinamentos que capacitem os usuários a trabalhar de forma a não infringir os pilares da Segurança da Informação

(Confidencialidade, Integridade e Disponibilidade), não apenas os colaboradores que fazem uso da rede, mas também os profissionais de TI.

Além de uma política bem definida e divulgada para todos os colaboradores, profissionais de segurança necessitam fazer escolher as ferramentas corretas que auxiliam na administração da rede e que devem ser implantadas seguindo as necessidades de cada ambiente. Essas ferramentas precisam estar atualizadas e receber monitoramento periódico a fim de identificar falhas que podem comprometer a segurança da companhia, podendo, em muitos casos, trazer prejuízo financeiro.

Diante de estudos e pesquisas realizados para elaboração deste artigo é possível notar que a Tecnologia da Informação torna-se cada vez mais um elemento essencial para o universo corporativo. Empresas que investem em Segurança da Informação podem economizar até US$ 1,6 milhão por ano [HP/Ponemon 2012a]. Esses números intensificam o conceito de que a Segurança da Informação deve ser considerada vital para o negócio de qualquer companhia de médio a grande porte.

Outras pesquisas citadas ao longo do artigo comprovam que existem diversos riscos relacionados à má utilização dos recursos de TI pelos colaboradores das empresas por todo o mundo.

O papel dos administradores de TI e Segurança da Informação é entender e prever as falhas humanas detectadas no processo de controle de vulnerabilidade e riscos e trata-las de forma proativa, assim como estar preparados para prováveis ocorrências e responder a elas no menor tempo possível, evitando assim, perda de capital.

AGRADECIMENTOS

Nossos sinceros agradecimentos são direcionados à todos aqueles que contribuíram direta e indiretamente para a conclusão de mais essa etapa de nossas vidas.

REFERÊNCIAS

Dantas, M. L. (2006). **Segurança da Informação – Uma Abordagem Focada em Gestão de Riscos**. Ed. Design.

Government Executive (2006). **Data on millions of vets stolen from VA employee's home**. http://www.govexec.com/federal-news, acessado em 28 de setembro de 2012.

HP/Ponemon (2011). **Second Annual Cost of Cyber Crime Study**. http://www.hpenterprisesecurity.com, acessado 14 de setembro de 2012.

HP/Ponemon (2012a). 2012 **Third Annual Cost of Cyber Crime Study** Results. http://www.hpenterprisesecurity.com, acessado em 16 de setembro de 2012.

HP/Ponemon (2012b). **The Growing Cost of Cyber Crime.** http://www.hpenterprisesecurity.com, acessado em 28 de setembro de 2012.

IDC Brasil (2012a). **IDC Brasil revela quais são os principais desafios que as empresas enfrentam na área de Segurança da Informação**. http://br.idclatin.com, acessado em 28 de agosto de 2012.

IDC Brasil (2012b). **Pesquisa da IDC revela que foram vendidos mais de 370 mil tablets no primeiro trimestre de 2012**. http://br.idclatin.com, acessado em 02 de setembro de 2012.

Instituto Qualibest (2008). **Internet no Trabalho vs Produtividade**. http://www.institutoqualibest.com.br, acessado em 03 de novembro de 2012.

ISO (2005). **Norma ISO 27001**. http://www.27000.org, acessado em 27 de agosto de 2012.

Kurose, J. F. (2010). **Redes de Computadores e Internet - Uma Abordagem Top-Down**. Ed. Pearson Addison Wesley.

Marques, P. E. P. C. (2011). **Tecnologia da Informação na Fundação Oswaldo Cruz**. Tese de mestrado, Escola Nacional de Saúde Pública Sérgio Arouca, Rio de Janeiro.

McAfee (2005). **Antivírus – Milhares de pessoas são vítimas de spyware diariamente**. http://home.mcafee.com, acessado em 13 de outubro de 2012.

Microsoft Technet (2012). **Respondendo à Incidentes de Segurança de TI.** http://technet.microsoft.com, acessado em 29 de setembro de 2012.

Microsoft (2012a). **Lista de Verificação de Segurança de Pequenas e Médias Empresas**. http://www.microsoft.com/brasil, acessado em 13 de outubro de 2012.

Microsoft (2012b). **O que é Software Antivírus?** http://www.microsoft.com, acessado em 13 de outubro de 2012.

Portal Fiocruz (2012). **Portal da Fundação Oswaldo Cruz**. http://portal.fiocruz.br, acessado em 28 de setembro de 2012.

Stamp, M. (2006). **Information Security – Principles and Practice**. Ed. John Wiley e Sons.

Symantec (1997). **Symantec – Vírus Infostealer**. http://www.symantec.com, acessado em 02 de setembro de 2012.

Symantec (2011). **Relatório sobre Segurança da Informação nas Empresas**. http://www.symantec.com, acessado em 13 de outubro de 2012.

Symantec (2012a). **Pesquisa sobre a Situação da Mobilidade – Resultados do Brasil**. http://www.symantec.com, acessado em 29 de setembro de 2012.

Symantec (2012b). **Relatório sobre Ameaças à Segurança na Internet.** http://www.symantec.com, acessado em 05 de setembro de 2012.

Symantec (2012c). **Symantec – Worm W32.Stikpid**. http://www.symantec.com, acessado em 02 de setembro de 2012.

Trend Micro (2010). **O ponto fraco da Segurança são os Funcionários?** http://smb.trendmicro.com.br, acessado em 02 de novembro de 2012.

Watkins, S. G. (2008). **An Introduction to Information Security and ISO 27001**. IT Governance Ltd.

Artigo submetido:23/08/2013

Artigo aceito: 07/03/2014