

Modelagem de Processos em Vulnerabilidades de Redes Sociais Usando BPMN

Rodrigo F. de Mattos, Evaldo de Oliveira da Silva¹

¹CES/JF – Centro de Ensino Superior de Juiz de Fora
Rua Halfeld, nº 1179 – Centro Juiz de Fora-MG

Bacharelado em Sistemas de Informação

{rodrigomattos7@yahoo.com.br, evaldo.oiveira@gmail.com}

Resumo. *O presente artigo descreve, inicialmente, o percurso histórico das redes sociais, ressaltando sua evolução e, ao mesmo tempo, apresenta algumas vulnerabilidades de segurança que podem causar sérios problemas a seus usuários. Também são apresentadas diversas ferramentas capazes de combater as vulnerabilidades citadas. Ao fim, é apresentado um diagrama baseado em modelagem de negócios que descreve o processo de combate às vulnerabilidades de acordo com as ferramentas que mais se enquadram em cada caso. O modelo pode orientar o usuário e também ser reutilizado em organizações distintas, possibilitando documentação dos processos de segurança da informação.*

Abstract. *This article describes, initially, the historical course of social networks, approaching its evolution and, at the same time, presents some security vulnerabilities that can cause serious problems to its users. Furthermore, this work presents different tools which are capable of avoiding these vulnerabilities. At the end, a diagram based on Business Process Management Notation (BPMN) is showed in order to describe the process of prevention the vulnerabilities which is agree with the tools that better fit in each process. The model can be reusable by different organizations and users which also can support documentation of information security processes.*

1. Introdução

Não há limites para o desenvolvimento tecnológico e, constantemente, surgem novos mecanismos de acesso e integração à informação, além das informações de diferentes fontes e origem de dados. A evolução tecnológica está permitindo uma grande interatividade com base na troca de informações, textos, imagens e sons. Pode-se observar também que esta evolução está relacionada à infraestrutura de redes de comunicação, possibilitando mais agilidade e transmissão de grandes volumes de dados.

As tecnologias de aplicações de software e redes avançadas de comunicação são amplamente utilizadas em ambientes residenciais e comerciais pelas organizações, mas podem permitir prejuízos no que se refere à segurança da informação. Entre estas tecnologias, é possível, inclusive, descrever vários aplicativos que se baseiam em funcionalidades utilizadas em redes sociais, os quais também permitem grande interação aproximando emissores e receptores de dados e também convivem com falhas de segurança e usuários que agem maliciosamente (NORRIS, 2012).

Com o uso da Internet por meio de seus diversos aplicativos e ambiente complexo, é possível identificar vulnerabilidades que podem prejudicar terceiros, e, inclusive, o próprio ambiente organizacional de uma instituição. Tais vulnerabilidades são descritas mais amplamente neste trabalho nas seções seguintes. São elas: a-) furto de identidade; b-) invasão de perfil; c-) uso indevido de informações; d-) sequestro e furto de bens; e e-) invasão de privacidade (CERT, 2016). Devido ao grande número de aplicações com base no ambiente Web, torna-se necessário modelar um conjunto de atividades que podem servir como gerenciamento de eventos de segurança, ou até mesmo como forma de atuar na mitigação das vulnerabilidades citadas.

Huber et al. (2009) destaca o crescente número de pessoas que usam sites de redes sociais para ampliar os relacionamentos entre si. As vantagens de utilização das redes sociais são evidentes e os serviços oferecidos são cada vez mais acessíveis. Porém, muitos usuários sofrem com a invasão de privacidade e roubo de informações, e os cuidados são negligenciados. Torna-se necessária uma abordagem de controle de vulnerabilidades para evitar a Engenharia Social que existe nas redes sociais da Internet, com base em tarefas, atividades e aplicações que permitam automatizar tais atividades a fim de mitigar as vulnerabilidades.

De acordo com Tiiu (2014), a Engenharia Social ataca as pessoas objetivando usar aspectos humanos como sentimentos para aplicar recursos técnicos de sabotagem dos controles de segurança a fim de extrair informações das aplicações dentro ou fora de organizações. Tiiu utiliza de modelagem de processos com base no BPMN (*Business Process Modeling Notation*) para apresentar um modelo que documenta as principais atividades da Engenharia Social dentro das organizações.

Com base nos trabalhos citados anteriormente, este artigo tem o objetivo de apresentar um conjunto de ferramentas que possam ser utilizadas no ambiente organizacional, a fim de combater as vulnerabilidades citadas em CERT (2016). Como resultado deste trabalho, é apresentado um modelo de processo de negócios com base no BPMN, que modela um conjunto de atividades a serem executadas utilizando as ferramentas pesquisadas.

O restante do artigo está organizado como segue. A Seção 2 apresenta o referencial teórico com os fundamentos conceituais que embasam este trabalho. A seção 3 aborda os principais elementos de modelagem de negócios usando o BPMN. A Seção 4 apresenta o modelo de negócios proposto para descrever as atividades e tecnologias necessárias para minimizar as vulnerabilidades discutidas. E, finalmente, a Seção 5 apresenta as considerações finais do trabalho.

2. Referencial Teórico

2.1. Redes Sociais dentro das Organizações

Os sistemas computacionais, tais como hardware, software e redes de comunicações, são aplicados e utilizados dentro das organizações de forma a apoiar a tomada de decisões e a interação entre pessoas envolvidas nos processos organizacionais. Nesse contexto, muitas aplicações de software têm sido amplamente utilizadas a fim de melhorar a interação entre as pessoas e enriquecer o processo de troca de informações.

Em um contexto mais geral, dentro da sociedade, Marteleto (2001, p.72) comenta que as redes sociais e suas aplicações de software representam um conjunto de

participantes autônomos, unindo ideias e recursos em torno de valores e interesses compartilhados. De acordo com Ciribeli e Paiva (2011, p. 69), “a utilização das redes sociais na Internet, antes mais comum em empresas de tecnologia e comércio eletrônico, tornou-se hoje um importante meio para se aproximar dos clientes e aumentar as vendas”. Os autores explicam que as redes sociais são um meio de facilitar as relações entre os usuários, derrubando barreiras físicas e culturais.

Ao abordar a importância das redes organizacionais, Capra (2002, p.267) relata que na era da informação as funções e processos sociais organizam-se cada vez mais em torno de redes. A organização em rede tornou-se um fenômeno social importante e uma fonte crítica de poder, já que a decisão em fazer é pessoal apesar de envolver um estudo multidisciplinar.

Ciribeli e Paiva (2011, p. 70) citam algumas vantagens da utilização de redes sociais pelas organizações, como o fato de poder “conhecer melhor os gostos dos seus clientes, manter contato permanente com eles e garantir a fidelidade deles”. Isso é possível graças ao crescimento da presença das redes sociais no dia-a-dia de grande parte dos consumidores. Assim, pode-se atingir milhões de consumidores de uma forma simples e rápida, garantindo um certo tipo de relação com os mesmos e uma divulgação mais ampla e eficaz.

Por outro lado, as empresas podem estar mais vulneráveis devido a sua alta exposição, como explicado por Cornachione (2010), que cita um caso de uma empresa que, após publicar uma campanha comercial, esta teve as falas trocadas por críticas à marca, causando uma repercussão negativa para a empresa.

Dessa forma, as redes sociais podem alavancar a imagem de uma empresa, mas também podem causar alguns efeitos colaterais, como a ampla divulgação de informações falsas, alcançando um impacto maior do que em outros tipos de mídia.

2.2. Vulnerabilidades das Tecnologias das Redes Sociais

Cavalcante (2013) considerou que o uso de programas maliciosos, email, websites, programas de transferência de informações, grupos de debate, redes sociais, sites de comércio eletrônico, entre inúmeros outros, além de vulneráveis, podem configurar crimes cibernéticos.

Não são somente as informações que tramitam nas redes sociais e na Internet como um todo que são alvos de ações perigosas aos usuários. As vulnerabilidades são constantes e comumente uma nova ferramenta ou instrumento de fraude ou invasão são reconhecidos, conforme relata CERT (2016, p. 18): “Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança”.

Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede. Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.

Para coibir a vulnerabilidade, CERT (2016) considera ainda que a Internet traz inúmeras possibilidades de uso, mas para aproveitar cada uma delas de forma adequada

é necessário que se tome medidas de segurança. Após conhecer os principais eventos de vulnerabilidade, o usuário deve manter-se atento às políticas de segurança adotadas para que não ocorram malefícios a sua integridade física ou virtual.

2.3. Principais Fatores de Vulnerabilidade

Dentre a vasta gama de ações contra o usuário, tanto na web quanto nas redes sociais, alguns riscos devem ser minimizados após atitudes de segurança e posicionamento frente à navegação e à troca de dados. Diferentemente de outros meios de comunicação ou acessibilidade virtual, as redes sociais possuem algumas características próprias, tais como “a velocidade com que as informações se propagam, a grande quantidade de pessoas que elas conseguem atingir e a riqueza de informações pessoais que elas disponibilizam” (CERT, 2016 p.87).

Os fatores acima mencionados juntamente com o alto índice de confiança em que as pessoas trocam informações por se tratar de uma rede de “amigos” tornaram essas redes um grande alvo de pessoas mal-intencionadas.

1) Furto de identidade:	Criação de falsos perfis (<i>fakes</i>). Por meio deles, as pessoas podem se passar por alguém com motivações criminosas.
2) Invasão de perfil:	Pode ocorrer meio de ataques de força bruta, do acesso a páginas falsas ou do uso de computadores infectados. Atacantes costumam fazer isto para, além de furto de identidade, explorar a confiança que a rede de contatos deposita e usá-la para o envio de <i>spam</i> e códigos maliciosos.
3) Uso indevido de informações	As informações divulgadas, além de poderem ser usadas para a criação de perfil falso, também podem ser usadas em ataques de força bruta, em golpes de Engenharia Social e para responder questões de segurança usadas para recuperação de senhas.
4) Sequestro e furto de bens:	Dados de localização podem ser usados por criminosos para descobrir uma rotina e planejar o melhor horário e local para abordar uma pessoa. Por exemplo: ao fazer <i>check-in</i> (se registrar no sistema) ao chegar a um cinema, um sequestrador pode deduzir que a vítima ficará lá por cerca de 2 horas (duração média de um filme) e terá este tempo para se deslocar e programar o sequestro ou furto.
5) Invasão de privacidade	Quanto maior a rede de contatos, maior é o número de pessoas que possui acesso ao que se divulga e menores são as garantias de que as informações não serão repassadas. Além disso, não há como controlar o que os outros divulgam sobre o dono da rede.

Tabela 1 – Quadro descritivo de principais vulnerabilidades. Adaptado pelo autor de CERT (2016, p.88)

Cavalcante (2013) relata que além dos crimes cibernéticos em si, é preciso se alertar contra outros riscos na rede, tais como a Engenharia Social. Segundo o autor, trata-se de um conjunto de habilidades utilizadas com o intuito de se conseguir que uma possível vítima forneça dados pessoais, realize uma tarefa ou execute um programa.

Em geral, para conquistar seu objetivo, se abusa da ingenuidade do alvo ou se procura ganhar a sua confiança, utilizando-se, por exemplo, de símbolos de instituições confiáveis, como órgãos públicos, grandes empresas, entre outros, para obter informações desejáveis ou invadir computadores.

2.4. Ferramentas que Combatem Vulnerabilidades

A partir do conhecimento sobre as vulnerabilidades citadas, são apresentadas a seguir algumas ferramentas que combatem tais problemas, bem como uma explicação sobre seu funcionamento.

2.4.1. Furto de Identidade

O furto de identidade pode ocorrer a partir da criação de perfis falsos (*fakes*), pois por meio deles as pessoas podem se passar por alguém com motivações criminosas. A seguir, são apresentadas ferramentas que previnem este tipo de ataque:

- **Findexif**

Para evitar problemas com perfis *fakes*, pode-se usar a ferramenta disponibilizada pelo site findexif.com, onde o usuário pode digitar o *link* de uma foto que será pesquisada pelo site. Este trará informações EXIF, ou seja, informações como o dispositivo com o qual se fez a foto, o lugar onde foi tirada, etc. Dessa forma, torna-se possível obter informações que ajudem a descobrir se a foto em questão pertence àquela pessoa ou se pode estar sendo usada uma identidade falsa. A ferramenta pode ser encontrada no *link* <http://www.findexif.com/> e seu uso é simples e gratuito, precisando apenas de acesso à Internet.

- **Foto Forensics**

A ferramenta, encontrada na página inicial do site <http://fotoforensics.com/>, funciona de forma semelhante ao Findexif. Basta fazer o upload de uma imagem ou fornecer o URL da mesma e o site retorna informações EXIF e também uma comparação que mostra quais detalhes foram editados ou adicionados na foto. O uso da ferramenta também é fácil, gratuito e é necessário apenas acesso à Internet.

- **Google SearchbyImage**

Outra maneira de analisar uma imagem é a pesquisa por imagem do Google. Para utilizá-la, é preciso apenas acessar o Google Imagens e clicar em "pesquisa por imagem" dentro da caixa de pesquisa. Feito isso, coloca-se o URL ou faz-se o *upload* da imagem a ser analisada. O Google retorna todas as informações que encontrar sobre a imagem como, por exemplo, links em que pode ser encontrada, imagens visualmente semelhantes, etc. Dessa forma, caso o fake esteja utilizando a imagem de outra pessoa, é fácil descobrir por meio do Google. O método é fácil, precisa apenas de acesso à Internet e pode ser utilizado em <https://www.google.com.br/imghp?hl=pt-PT&tab=wi&ei=-lvsV83UGIOPwgTds5mwBw&ved=0EKouCBIoAQ>.

- **TinEye**

Assim como as anteriores, a ferramenta funciona de forma simples. Basta fazer o upload da imagem a ser analisada ou fornecer seu URL. O site retorna todos os links onde essa imagem pode ser encontrada. Seu uso é gratuito (exceto para fins comerciais) e pode ser feito por meio do link <http://tineye.com/> ou por meio de uma extensão para navegador que pode ser adquirida no mesmo endereço. O usuário também pode criar uma conta no site para poder visualizar suas pesquisas posteriormente.

- **JPEGSnoop**

O JPEGsnoop é um programa que pode ser usado apenas no sistema operacional Windows e que cumpre a função de fornecer informações não somente sobre imagens, mas também acerca de arquivos como vídeos, documentos em pdf, entre outros. Ele possibilita saber se uma imagem foi alterada, descobre com qual programa foi produzida, encontra erros em arquivos corrompidos, etc. A ferramenta é gratuita, leve e não precisa de instalação, mas seu uso pode ser um pouco complicado para um usuário com pouco conhecimento sobre imagens. O download do programa pode ser feito no link <http://jpegstnoop.softonic.com.br/>.

- **Fakespot**

Para quem compra no site Amazon e não quer ser enganado por clientes fake que recebem benefícios dos vendedores em troca de avaliações positivas em seus produtos, a ferramenta Fakespot fornece a porcentagem de avaliações falsas no produto a ser analisado. Basta que o interessado forneça à ferramenta o link do produto. A ferramenta analisa as avaliações positivas vendo se estes clientes realmente compraram o produto e correlaciona com outros dados de avaliações falsas. Fakespot está disponível no link <http://fakespot.com/>, mas também pode ser usada como extensão para o navegador Google Chrome, facilitando seu uso, pois assim as análises são feitas já durante a navegação no site da Amazon. O uso da ferramenta é simples e gratuito.

- **SmartScreen**

Para evitar ataques de phishing em redes sociais, e-mails e outros sites, existem algumas ferramentas disponibilizadas pela Microsoft. No navegador Internet Explorer, o nome do domínio na barra de endereços é ressaltado na cor preta para ajudar a identificar a identidade de um site. Também existe um filtro chamado SmartScreen neste navegador que informa quando o site é potencialmente perigoso. A tecnologia SmartScreen também separa e-mails perigosos de e-mails legítimos no Outlook, webmail gratuito da Microsoft. O filtro de lixo eletrônico do Outlook analisa os e-mails para ver se eles contêm características comuns a golpes de phishing. As mensagens avaliadas como suspeitas são enviadas para a caixa de lixo eletrônico e quaisquer links ou anexos são bloqueados para garantir a segurança do usuário, que pode desfazer o procedimento caso julgue a mensagem como confiável. É possível saber mais sobre a ferramenta acessando o site da Microsoft pelo link <https://support.microsoft.com/pt-br/help/17443/windows-Internet-explorer-smartscreen-filter-faq>.

2.5.2. Invasão de Perfil

A invasão de perfil pode ocorrer por meio de ataques de força bruta, do acesso a páginas falsas ou do uso de computadores infectados. Atacantes costumam fazer isto para, além de furto de identidade, explorar a confiança que a rede de contatos deposita e usá-la para o envio de *spam* e códigos maliciosos. A seguir, são citadas algumas ferramentas que atuam na prevenção deste tipo de ataque.

- **Hootsuite – Social Media Security**

A empresa canadense Hootsuite fornece uma ferramenta de gerenciamento de redes sociais que se mostra útil para empresas que lidam com este meio de comunicação. Com essa ferramenta, é possível conceder aos funcionários o acesso às redes sociais da empresa sem necessidade de compartilhar senhas, manter seguras as senhas de WiFi mesmo em dispositivos que o utilizem, monitorar atividades nas contas, recebendo notificações em tempo real caso haja alguma atividade suspeita, garantir que dados privados não sejam compartilhados, etc. A empresa possui um plano livre básico (até 3 perfis em redes sociais), um plano pro (até 50 perfis) e um plano business (até 50 perfis, mas com análises em tempo real, suporte prioritário, etc.). A ferramenta pode ser encontrada no link <https://hootsuite.com/pt/planos/enterprise>.

- **Metasploit**

A Metasploit, ferramenta mais popular no que se refere a testes de invasão de perfil, é um framework que conta com testes personalizados e procura vulnerabilidades em sistemas operacionais e aplicações. A ferramenta permite verificar a segurança de máquinas, simulando ataques antes que estes aconteçam de verdade. O uso da ferramenta exige algum conhecimento tecnológico, é gratuito em sua versão básica e seu download pode ser feito através do link <https://www.rapid7.com/products/metasploit/download.jsp>.

- **BelkasoftEvidence Center**

Para saber se um perfil foi invadido, pode-se usar uma ferramenta paga chamada BelkasoftEvidence Center, encontrada na suíte de produtos da Belkasoft. Com essa ferramenta, é possível acessar conversas, arquivos e outros registros ou atividades de um usuário por meio de seu equipamento (laptop, smartphone, etc.). A ferramenta faz uma pesquisa textual completa a fim de coletar evidências e apresentar uma linha do tempo com as atividades encontradas. Dessa forma, o usuário pode descobrir se houve invasão apenas verificando se não reconhece alguma das atividades. A ferramenta não precisa de Internet durante sua utilização e pode ser encontrada no endereço <https://belkasoft.com/ec>.

- **BurpSuite**

Almejando trabalhar na prevenção das invasões, pode-se testar as aplicações web que o usuário deseja utilizar. Para isso, pode-se fazer uso da ferramenta BurpSuite, que realiza testes de segurança fazendo mapeamentos e análises que lhe permitem inferir sobre a vulnerabilidade da segurança da aplicação analisada. A ferramenta possui uma versão grátis e uma versão paga. Esta última possui funcionalidades como a possibilidade de

salvar os trabalhos para continuar mais tarde e algumas ferramentas mais avançadas de análise. O download da ferramenta é feito no endereço <https://portswigger.net/burp/download.html>.

2.5.3. Uso Indevido de Informações

As informações que são divulgadas, além de poderem ser usadas para a criação de perfil falso, também podem ser usadas em ataques de força bruta, em golpes de Engenharia Social e para responder questões de segurança usadas para recuperação de senhas.

- **EmailExposureCheck**

Uma organização chamada knowbe4 trabalha oferecendo treinamentos sobre segurança para funcionários de empresas. Além dos treinamentos, ela oferece algumas ferramentas gratuitas para testar a segurança digital destas empresas. Uma destas ferramentas é a EmailExposureCheck(EEC), que verifica quais informações da empresa estão disponíveis publicamente e onde elas se encontram. Assim, é possível encontrar sites externos ou diretórios que contenham endereços de e-mail, por exemplo, o que poderia resultar em ataques ou envios de spam por e-mail. Sabendo a localização dessas informações, é possível tomar medidas de precaução ou buscar a remoção delas. A ferramenta só funciona a partir do domínio próprio da empresa (as pesquisas são feitas a partir desse domínio). O uso grátis é oferecido para apenas um teste onde o usuário fornece o domínio e a Knowbe4 lhe retorna um e-mail com as informações. Pode-se encontrar essa ferramenta no link www.knowbe4.com/email-exposure-check/.

2.5.4. Sequestro e Furto de Bens

Dados de localização podem ser usados por criminosos para descobrir uma rotina e planejar o melhor horário e local para abordar uma pessoa. Por exemplo: ao fazer *check-in* (se registrar no sistema) ao chegar a um cinema, um sequestrador pode deduzir que a vítima ficará lá por cerca de 2 horas (duração média de um filme) e terá este tempo para se deslocar e programar o sequestro ou furto.

Para evitar este tipo de ataques, o melhor a fazer é estar atento à definição de privacidade das publicações. O usuário deve selecionar a opção “apenas amigos” no que diz respeito às visualizações da publicação em questão (especialmente aquelas que contêm informações sobre a localização do usuário ou de seus familiares) e garantir que entre seus amigos não haja um desconhecido ou alguém que não seja de sua confiança. Para isso, pode-se verificar a existência de perfis falsos entre a lista de amigos ou seguidores. O tópico seguinte fornece algumas dicas para essa verificação.

- **Como reconhecer *fakes***

De acordo com a empresa especializada em segurança tecnológica Barracuda Networks, a maioria dos perfis *fakes* segue as seguintes características:

- ✓ A maioria dos perfis *fakes* afirma serem mulheres e bissexuais;
- ✓ Geralmente possuem muitos amigos/seguidores;
- ✓ Não costumam fazer muitas postagens/atualizações de status;

Dessa forma, caso o usuário não conheça algum amigo ou seguidor, não é conveniente manter conversas ou deixar visíveis informações pessoais, fotos de família, dados de localização, etc. O ideal a se fazer, para garantir segurança nas redes sociais, é excluir amigos suspeitos.

Para auxiliar o usuário na identificação de perfis não confiáveis, pode-se fazer uso das ferramentas citadas anteriormente, no item que discorre sobre furto de identidade. Além disso, é importante ter cuidado ao utilizar computadores compartilhados, pois caso o usuário se esqueça de apagar senhas, dados de preenchimento de formulários (especialmente aqueles que contêm endereços, CPF, número de telefone, etc.), alguma pessoa mal-intencionada pode apropriar-se dos dados e utilizá-los de forma criminosa.

2.5.5. Invasão de Privacidade

Quanto maior a rede de contatos, maior é o número de pessoas que possui acesso ao que se divulga, e menores são as garantias de que as informações não serão repassadas. Além disso, não há como controlar o que os outros divulgam sobre o dono da rede.

Windows 10

Uma das características do Windows 10 é que o usuário é constantemente monitorado pela Microsoft. Suas ações são enviadas por meio de relatórios para a empresa, o que é considerado por muitos como invasão de privacidade, embora a empresa argumente que essa funcionalidade serve apenas para melhorar a experiência do usuário. Existem muitas formas de negar o envio de tais relatórios, mas, além de trabalhoso, o acesso a estas opções nem sempre é direto. Assim, foram criadas algumas ferramentas para evitar possíveis transtornos com privacidade no sistema operacional mencionado.

- **Destroy Windows 10 Spying**

O Destroy Windows 10 Spying é um exemplo de ferramenta que, além de fazer ajustes no sistema removendo e bloqueando o monitoramento da Microsoft, ainda permite remover aplicativos padrão da Microsoft e instalar outros que a empresa oferecia em sistemas operacionais anteriores, como o visualizador de imagens do Windows. O Destroy Windows 10 Spying é gratuito, não precisa de instalação e seu uso é simples. Para utilizá-lo e obter um guia com maiores explicações, pode-se acessar o link <https://kmspico.org/2015/08/09/destroy-windows-10-spying-1-4-3-update-guide/>.

- **Disable Windows 10 Tracking**

A ferramenta de código aberto Disable Windows 10 Tracking também auxilia o usuário do Windows 10 na preservação de sua privacidade, pois oferece a possibilidade de desativar serviços de rastreamento feitos pelo sistema e alterar configurações de registro, impedindo que aplicativos recolham informações sobre o usuário e enviem relatórios à Microsoft. Seu download e uso são simples e gratuitos. O programa apresenta uma lista de recursos de rastreamento e o usuário determina quais informações deseja manter privadas. É preciso apenas que o usuário realize estas ações no modo de administrador. O programa pode ser obtido no link <https://github.com/10se1ucgo/DisableWinTracking/releases>.

3. Modelagem de Processos de Negócios

Para facilitar a compreensão do funcionamento das ferramentas apresentadas com o objetivo de mitigar as vulnerabilidades, utilizou-se a notação para modelagem de processos de negócios proposto pelo BPMI (*Business Process Model Initiative*) (BPMI, 2016). O modelo foi criado por meio da ferramenta *Bizagi* (BIZAGI, 2016), representando um passo a passo que pode ser seguido pelo usuário caso identifique alguma vulnerabilidade em um site, rede social, e-mail ou até mesmo um sistema operacional, e queira investigá-la para tomar medidas corretivas ou preventivas em relação a sua segurança.

O Software Bizagi, de acordo com Flores e Amaral (2014, p. 2), “é uma ferramenta livre, específica para o mapeamento de processos e que utiliza como base a notação BPMN, possibilitando que o analista desenvolva o desenho do processo e detalhe todas as tarefas pertencentes aos processos”. Dessa forma, a ferramenta é ideal para representar processos, detalhando as atividades que devem ser executadas para que se alcance um determinado objetivo.

Por meio de sua linguagem padrão, qualquer pessoa que seja conhecedora da simbologia utilizada é capaz de entender um diagrama criado na ferramenta Bizagi. Assim, sua utilização neste trabalho foi importante para garantir o entendimento do leitor e de possíveis usuários do modelo.

A modelagem de processos de negócios, segundo Tiiu (2014, p. 3), é uma forma de apresentar processos para que possam ser utilizados, analisados e aperfeiçoados. De acordo com Hammer e Champy (1994), processos são grupos de atividades que são realizadas de maneira lógica a fim de atingir um objetivo específico. Com o BPMN, essas atividades são apresentadas de forma simples, para que qualquer interessado possa realizá-las de forma rápida e eficaz, sem se esquecer de algum passo importante, além de poder verificar todo o processo de forma ampla, podendo identificar falhas rapidamente.

Assim, a modelagem apresentada na Seção 4 deste trabalho mostra os caminhos que o usuário deve seguir caso identifique falhas na segurança, guiando-o na prevenção de vulnerabilidades às quais pode estar exposto na utilização de diversos tipos de tecnologias, mostrando um plano de ação simples e eficaz no tratamento dessas vulnerabilidades e até mesmo fornecendo orientações necessárias caso o usuário esteja sendo vítima de algum crime relacionado. Abaixo segue a Figura 1, que apresenta os principais elementos para modelagem de processos de negócios de acordo com o BPMN.

Conhecendo os principais elementos contidos em um diagrama de modelagem de negócios, é possível entender o modelo de ação apresentado no capítulo 4 deste trabalho e todos os passos sugeridos para tratar os casos de vulnerabilidades de segurança.








	Indica o início ou fim do processo
	Indica cada atividade que precisa ser executada
	Indica um ponto de tomada de decisão
	Indica a direção do fluxo
	Indica os documentos utilizados no processo
	Indica uma espera
	Indica que o fluxograma continua a partir desse ponto em outro círculo, com a mesma letra ou número, que aparece em seu interior

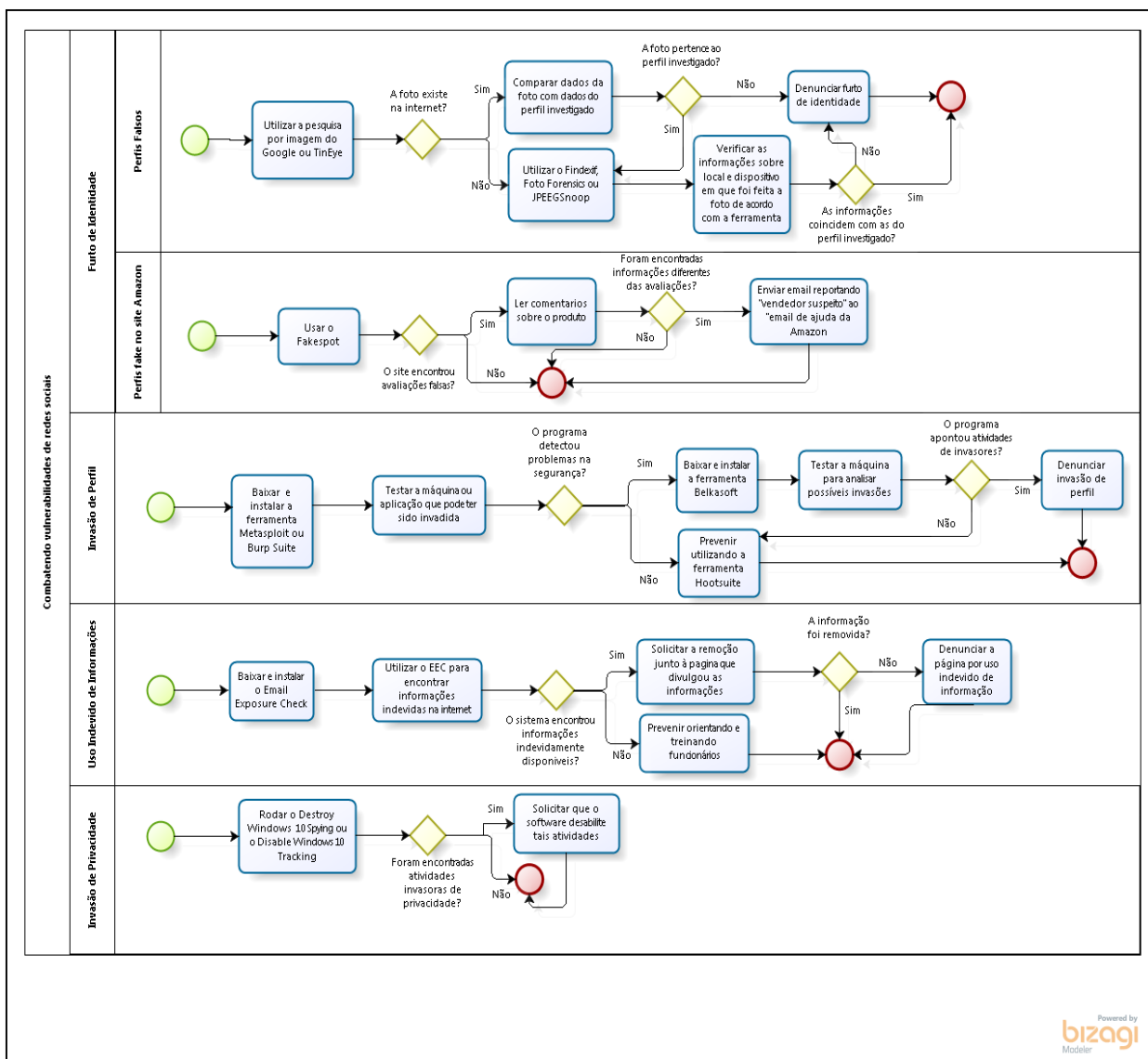
Figura 1 – Elementos para modelagem de processos de acordo com o BPMN

Fonte: BPMN (2016)

4. Modelagem de Processos em Vulnerabilidades de Redes Sociais Usando BPMN

O modelo da Figura 2 a seguir mostra algumas situações de falhas de segurança e o processo, isto é, a forma como se deve agir, em cada um dos casos. O modelo foi elaborado a partir de estudos feitos por meio de fontes como os sites oficiais das ferramentas e sites especializados em tecnologia e segurança cibernética. A partir desses estudos, foi possível entender a utilidade e o funcionamento de cada ferramenta podendo, assim, criar um resumo prático para que qualquer pessoa interessada possa utilizar como guia.

De maneira geral, após baixar ou acessar o site da ferramenta indicada para o problema em questão, o usuário deve seguir o procedimento detalhado no fluxograma, para que possa identificar possíveis falhas de segurança. De acordo com o resultado obtido, deve-se adotar uma ação específica para o caso, como pode ser observado no modelo. Após executar tal ação, caso o problema seja resolvido, encerra-se o processo. Caso contrário, deve-se tomar uma ação mais drástica visando à proteção do usuário. Se houver suspeita de uma ação criminosa, o usuário pode denunciar o autor e solicitar as medidas cabíveis, como remoção de informações privadas e até mesmo indenizações.



Powered by bizagi Modeler

Figura 2 – Modelo de Ação em Caso de Detecção de Falhas de Segurança

Fonte: Ferramentas analisadas (2016)

5. Considerações Finais

O artigo discutiu a presença cada vez maior das redes sociais tanto no âmbito pessoal como no profissional, ressaltando seu percurso histórico, suas vantagens e desvantagens. Também foi mostrado que, graças ao crescimento da tecnologia, tem aumentado também a incidência de crimes virtuais no que se refere à violação de dados e indivíduos mal-intencionados no meio internauta, revelando os perigos proporcionados pelos usuários que se valem do conhecimento técnico para conseguir benefícios prejudicando outros.

Foram apresentados neste trabalho alguns tipos de vulnerabilidades de segurança encontrados na Internet, de forma a apresentar possibilidades de crimes que possam ser

praticados nesse meio. Em contrapartida, foram apresentadas diversas ferramentas e dicas para combate dessas vulnerabilidades.

Diante da quantidade de ferramentas disponíveis para o combate das vulnerabilidades das redes sociais, foram escolhidas algumas delas para elaboração deste trabalho devido a limitações de tempo e conveniência. Estudos futuros podem abordar de maneira mais profunda o estudo destas ferramentas, bem como desenvolver outros tipos de projetos que possam contribuir para melhorias deste campo de estudo.

Ao fim, foi apresentado um modelo de negócios elaborado com o intuito de auxiliar usuários interessados em precaver ou corrigir situações de riscos de segurança. Dessa forma, é possível dizer que este estudo é capaz de proporcionar ao leitor um melhor entendimento acerca da segurança no meio virtual, bem como auxiliar nas ações de proteção à segurança do leitor enquanto usuário das redes sociais.

Referências

- BELKASOFT. Site oficial do desenvolvedor. Disponível em <<https://belkasoft.com/ec>>. Acesso em 23 de ago de 2016.
- BIZAGI. Bizagi. Disponível em: <http://www.bizagi.com/pt/>. Acesso em: 12 de out de 2016.
- BPMN. BPMN Quick Guide. Disponível em: <http://www.bpmnquickguide.com/view-bpmn-quick-guide/>. Acesso em 15 de outubro de 2016.
- BPMI. Object Management Group Business Process Model and Notation. Disponível em: <http://www.bpmn.org/>. Acesso em 12 de out de 2016
- CAPRA, Fritjof. As conexões ocultas: ciência para uma vida sustentável. São Paulo: Cultrix, 2002. Disponível em <https://books.google.com.br/books>.
- CAVALCANTE, Waldek Fachinelli. Crimes cibernéticos: investigação e ameaças na Internet. Revista Jus Navigandi, Teresina, ano 18, n. 3782, 8 nov. 2013. Disponível em: <<http://jus.com.br/artigos/25743>>. Acesso em: 8 de ago de 2015
- CERT.br. Cartilha de segurança para Internet. 2016. Disponível em: <<http://cartilha.cert.br/>>. Acesso em: 26 de nov de 2016.
- CIRIBELI, João Paulo, PAIVA, Victor Hugo Pereira. Redes e mídias sociais na Internet: realidades e perspectivas de um mundo conectado. Revista Mediação, Belo Horizonte, v. 13, n. 12, jan./jun. de 2011.
- CORNACHIONE, Daniella. As empresas querem entrar. Época, São Paulo, n. 628, p. 92-94, 31 mai. de 2010.
- FAKESPOT. Site oficial da ferramenta. Disponível em <<http://fakespot.com/>>. Acesso em 23 de ago de 2016.
- FINDEXIF. Site oficial da ferramenta. Disponível em <<http://www.findexif.com/>>. Acesso em 23 de ago de 2016.
- FLORES, Evandro G., AMARAL, Marisa M. Mapeamento de Processos Utilizando a Metodologia BPM Uma ferramenta de suporte estratégico no desenvolvimento de sistemas em uma Instituição Federal de Ensino Superior. Anais do EATI. 2014.

- FOTO FORENSICS. Site oficial da ferramenta. Disponível em <<http://fotoforensics.com/>>. Acesso em 23 de ago de 2016.
- GITHUB. Site de downloads. Disponível em <<https://github.com/10se1ucgo/DisableWinTracking/releases>>. Acesso em 23 de ago de 2016.
- GOOGLE. Pesquisa de imagens. Disponível em <<https://www.google.com.br/imghp?hl=pt-PT&tab=wi&ei=lvsv83UGIOPwgTds5mwBw&ved=0EKouCBIoAQ>>. Acesso em 23 de ago de 2016.
- HAMMER, Michael; CHAMPY, James. Reengineering the Corporation. New York: HarperBusiness, 1994.
- HOOTSUIT. Site oficial da ferramenta. Disponível em <<https://hootsuite.com/pt/planos/enterprise>>. Acesso em 23 de ago de 2016.
- HUBER, Markus, et al. "Towards automating social engineering using social networking sites." Computational Science and Engineering, 2009. CSE'09. International Conference on. Vol. 3. IEEE, 2009.
- JPEGSNOOP. Site oficial da ferramenta. Disponível em <<http://jpegsnoop.softonic.com.br/>>. Acesso em 23 de ago de 2016.
- KMSPICO. Site oficial do desenvolvedor. Disponível em <<https://kmspico.org/2015/08/09/destroy-windows-10-spying-1-4-3-update-guide/>>. Acesso em 23 de ago de 2016.
- KNOWBE4. Site oficial do desenvolvedor. Disponível em <www.knowbe4.com/email-exposure-check/>. Acesso em 23 de ago de 2016.
- MARTELETO, Regina Maria. Análise de redes sociais: aplicação nos estudos de transferência da informação. Ciência da Informação, Brasília, v. 30, n. 1, p. 71-81, jan./abr. 2001.
- MICROSOFT. Perguntas frequentes sobre o filtro SmartScreen. Disponível em <<https://support.microsoft.com/pt-br/help/17443/windows-Internet-explorer-smartscreen-filter-faq>>. Acesso em 24 de ago de 2016.
- NORRIS, I. N. (2012). Mitigating the effects of doxing (Doctoral dissertation, Utica College).
- PORTSWIGGER. Site oficial do desenvolvedor. Disponível em <<https://portswigger.net/burp/download.html>>. Acesso em 23 de ago de 2016.
- RAPID7. Site oficial do desenvolvedor. Disponível em <<https://www.rapid7.com/products/metasploit/download.jsp>>. Acesso em 23 de ago de 2016.
- TIIU, Mamers. Application of Security Risk-oriented BPMN to Manage Social Engineering Risks. 2014. Disponível em: <https://courses.cs.ut.ee/MTAT.03.246/2013.../essay04-2014.pdf>. Acesso em 12 de out de 2016.
- TIN EYE. Site oficial da ferramenta. Disponível em <<http://tineye.com/>>. Acesso em 24 de ago de 2016.