Revista FATEC Sebrae em debate: gestão, tecnologias e negócios
Vol. 3 | Nº. 5 | Ano 2016 | ISSN: 2358-9817

PRINCIPAIS FORMAS DE ATAQUE E PREVENÇÃO À INFORMAÇÃO NO AMBIENTE DA INTERNET

ROBSON ANTONIO MOREIRA

Mestre em Gerenciamento de Sistemas de Informação
Faculdade de Tecnologia de Jahu

FATEC Sebrae – Faculdade de Tecnologia Sebrae - CEETEPS – Centro Estadual de Educação Tecnológica Paula Souza – São Paulo, Brasil.

Revista FATEC Sebrae em debate gestão, tecnologias e negócios

Editor Geral
Prof. Dr. Mário Pereira Roque Filho

Organização e Gestão
Prof. Ms. Clayton Pedro Capellari

Correspondência
Alameda Nothmann, nº 598 Campos Elíseos, CEP 01216-000 São Paulo – SP, Brasil.
+55 (11) 32240889 ramal: 218
E-mail: f272dir@cps.sp.gov.br

Resumo

O presente artigo tem como objetivo apresentar a o valor da informação e, a importância da Segurança da Informação para organizações e pessoas que utilizam a rede mundial de computadores: a Internet. Atualmente, a informação é um ativo de altíssimo valor. Ela representa valor, e consequentemente, contribui diretamente para a geração de lucro, é possível afirmar então que a informação é um bem, um ativo da organização, e como tal deve ser preservado e protegido como os demais bens. A indisponibilidade da informação traz prejuízos financeiros para as empresas e podem causar danos irreparáveis as pessoas. Diante dessa realidade é extremamente necessário ter conhecimento das ameaças e vulnerabilidades que todos sofrem quando acessam a Internet. No ano de 2015 mais de 3,2 bilhões de pessoas compartilharam e tiveram acesso às informações através desse ambiente. O acesso à informação é cada vez maior e mais fácil a todos. Por esta razão, a prevenção é a melhor forma de proteção. Conhecer como os atacantes, os famosos “hacker” e sua maneira de agir facilita a proteção, minimiza os ataques e mitigando as vulnerabilidades.

O Artigo apresenta as principais modalidades de ataques utilizadas através da Internet e, as medidas de segurança indispensáveis para obter segurança. Conclui-se que a utilização e compartilhamento de mecanismos de segurança são extremamente úteis e relevantes para todos da sociedade.

Palavras-chave: informação; internet; segurança da informação.

Abstract

This piece aims to show the value of information and the importance of Information Security for companies and people that use the World Wide Web: the Internet. Currently, information is a high cost value. As the Internet represents value, and though, it contributes to profit generation directly, it is possible to affirm that information is a property, an asset of the organization, and as such, it must be unspoiled and protected like any other goods. The information unavailability puts at a financial disadvantage to the companies and may cause irreparable damage to people. Towards such reality it is extremely necessary to know the threats and the weak points that everyone is submitted when accessing the Internet. In 2015, more than 3.2 billion people shared and had access to information by such environment. The access to information is wider and easier to everyone. For this reason, prevention is the best way to be protected. Knowing the attackers, the famous 'hacker' and how they act facilitates protection, diminishes their attacks, and mitigates vulnerabilities. The paper presents the main types of attacks used in the Internet, besides indispensable security actions to be safe. Then it is concluded that the use of information sharing is extremely useful and relevant for society; however, in a virtual environment, security is more than a need; it is an ally in protection and validity of the most precious value possed: information.

Keywords: INFORMATION; INTERNET; INFORMATION SECURITY

Introdução

A informação é um elemento fundamental para a raça humana. A informação permitiu descobertas com o fogo, a roda e, outras comuns no nosso dia a dia. Independente do nível de interação que a sociedade tem com a informação ela é parte das nossas vidas. O nível de conhecimento é resultado do compartilhamento das informações de geração para geração. Esse compartilhamento é ainda mais acelerado na sociedade atual. (PONTES, 2012)

Na atual sociedade, a informação é um recurso muito importante e indispensável. A informação é um ativo valioso e, deve ser tratada como bem estratégico para as empresas. A informação é um importante fator para a tomada de decisão de empresas e das demais pessoas que dependem dela. Essa sociedade pode desfrutar de uma quantidade imensurável de informação que há alguns anos atrás era um item escasso. De acordo como World Bank (2016) as tecnologias digitais tem se disseminado rapidamente nos países em desenvolvimento. Índices próximos, por exemplo, aos da melhoria do abastecimento de água. Em outras palavras, pode-se concluir que a informação está chegando mais rapidamente às pessoas do que o fornecimento de água. Mas, este rápido acesso à informação tem um preço para sua efetiva utilização. Sem o conhecimento sobre as formas de atuação dos criminosos virtuais e, as modalidades essenciais de garantia à segurança da informação tal facilidade e disponibilidade não seriam possíveis. Infelizmente, em razão da facilidade de utilização, muitas pessoas utilizam a internet para obtenção e compartilhamento da informação sem as devidas medidas de segurança. A prevenção é e continuará sendo a melhor maneira de evitar prejuízos e danos que podem se tornar irreparáveis.

1.1 Objetivo

O objetivo deste Artigo é apresentar através de uma revisão bibliográfica a atual importância da informação na sociedade. Alinhado a essa importância e, do compartilhamento da informação através de meios digitais – essencialmente a Internet - analisando as principais formas de ataques e as medidas fundamentais para garantir segurança da informação.

1.2 Metodologia

A metodologia utilizada para a elaboração deste Artigo é denominada de revisão bibliográfica ou revisão de literatura. Essa modalidade de pesquisa se vale de publicações científicas em periódicos, livros, anais de congresso etc. não se dedicando de coleta de dados *in* natura, porém não configura em simples transição de ideias. (BRASILEIRO, 2013)

2 Revisão Bibliográfica

Para Kim e Solomon (2014) a Internet ou *World Wide Web* é a grande teia de alcance mundial que conecta, na atualidade, mais de três bilhões de usuários. É neste ciberespaço ou simplesmente Internet que as páginas web e uma enorme quantidade de documentos nos mais formatos digitais conectam pessoas independentemente da distância.

De acordo com o World Bank (2016) as tecnologias digitais (internet, smartphones) e todas as outras ferramentas para coligir, armazenar, analisar e compartilhar informações digitalmente – disseminaram-se rapidamente. Um maior número de domicílios nos países em desenvolvimento dispõe mais de telefone celular do que de acesso à eletricidade ou à água potável, e quase 70% do quinto mais pobre da população da população em países em desenvolvimento têm telefone celular. O número de usuários da Internet mais do que triplicou em uma década – de um bilhão em 2005 para cerca de 3,2 bilhões no final de 2015. Indiscutivelmente, mais empresas, pessoas e governos estão ainda mais conectados.

Infelizmente, a conexão através deste ciberespaço (Internet) abre as portas para muitos sujeitos de pouca confiabilidade e, que querem encontrá-lo e roubar dados dos usuários. Todos os computadores conectados à Internet estão constantemente em risco. Proteger as informações dos invasores é mais que uma necessidade é deve de todo usuário. Afinal, a internet e as tecnologias de informação utilizadas estão em

constantes modificações o que as tornam vulneráveis sem a devida atenção a métodos de prevenção.

Cibersegurança ou segurança na Internet é dever de cada governo que deseja garantir a própria segurança nacional. É reponsabilidade de cada organização e é função de cada um proteger seus próprios dados. (KIM; SOLOMON, 2014)

Os componentes dessa rede mundial – Internet – não são automaticamente seguros e incluem cabeamento, redes físicas, sistemas operacionais e aplicativos de software que os computadores e dispositivos usam para se conectar a Internet. (KIM; SOLOMON, 2014)

A Internet é o novo local para se reunir, socializar e compartilhar ideias. Bater papo como os amigos, famílias e contatos de negócios foram facilitados. Mas há um perigo: você não sabe realmente quem é a pessoa do outro lado da conexão. Mentirosos e ladrões podem facilmente esconder suas identidades. Embora a Internet lhe ofereça acesso na ponta dos dedos a pessoas e informações, ela também traz muitos riscos e ameaças. (KIM; SOLOMON, 2014).

Uma guerra de segurança da informação se alastra. O campo de batalha é a Internet, os inimigos estão em toda parte e próximos – afinal a Internet permite essa proximidade, embora fisicamente distantes. (KIM; SOLOMON, 2014).

Em tempos de informação digital – trafegando pela internet – essa quantidade tem indicadores de extrema grandiosidade. Diariamente, são postadas mais de 186 milhões de fotos na rede social Instagram, mais de 8,8 bilhões de vídeos assistidos no Youtube, a quantidade de e-mails enviados supera 207 bilhões, 4,2 bilhões de buscas são realizadas apenas pelo Google além de 36 milhões de compras efetuadas pela Amazon. (WORLD BANK, 2016)

Por esta razão, que antes de identificar os motivos dos ataques virtuais é extremamente importante entender o que os “inimigos” almejam, ou seja, a informação e a sua importância que tem para todos nós.

2.1 O valor da Informação

Campos (2014) destaca que o termo informação teve destaque e ganhou importância na década de 1960. Foi nesta década que surgiu uma nova área na ciência denominada ciência da informação. Mas, foi na década de 1980 com o advento da Internet que o tema voltou a se posicionar em destaque. Desde então, a informação para o indivíduo, para as organizações e sociedade foi amplamente pregada. Nonaka cita Bateson esclarecendo que “a informação consiste em diferenças que fazem diferença”. Assim, a informação possui significado e causa impacto em grau menor ou maior, tornando-a elemento essencial da extração e criação do conhecimento.

A informação é um ativo que, como qualquer outro ativo de extrema importância tem um valor para a organização. Diante dessa importância é necessário a sua segurança. A segurança da informação protege a informação de diversos tipos de ameaças garantindo a continuidade dos negócios e minimizando os danos e maximizando o retorno dos investimentos e das oportunidades. (FERREIRA, 2003)

Uma vez que a informação representa valor, e consequentemente, contribui diretamente para a geração de lucro, é possível afirmar então que a informação é um bem, um ativo da organização, e como tal deve ser preservado e protegido como tal os demais ativos da organização, se é que se pretende atingir o sucesso desejado. (CAMPOS, 2014)

Segundo Campos (2014) a informação é o elemento essencial para todos os processos de negócio da organização, sendo um ativo de grande valor. O mesmo autor completa que da mesma forma que a informação é importante para as empresas, os meios que dão suporte, que a mantém e permite que existam também são. Nesta situação encontram-se: equipamentos e dispositivos de tecnologia da informação ou em cadernos e manuais de procedimentos. A informação permeia toda a organização, apoiando seus processos de diversas formas, em diversos meios. É possível encontrar a informação em forma escrita ou impressa armazenada em arquivos ou mídias digitais.

Diante de tal importância diz-se que se vive a era da informação. Na sociedade da informação, ao mesmo tempo em que as informações são os principais ativos da organização, estão também em constante risco, como nunca estiveram antes. Com

isso, a segurança da informação tornou-se ponto crucial para a sobrevivência das organizações. (FERREIRA, 2003)

A informação, na atualidade, é mais do que um simples ativo: é um ativo valioso. Essas informações valiosas podem auxiliar as pessoas em suas organizações a realizar tarefas de forma mais eficiente e eficaz. (STAIR; REYNOLDS, 2015)

Para entender como tornar computadores mais seguros, primeiramente deve-se entender o que são riscos, ameaças e vulnerabilidades.

2.2 Riscos, Ameaças e Vulnerabilidades à Informação.

Risco é a probabilidade de que algo ruim aconteça a um bem, a exposição a algum evento que tenha efeito sobre um bem. No contexto de segurança da Tecnologia da Informação (TI), um bem pode se um computador, um banco de dados ou uma informação. Como exemplo de risco inclui-se: a) Perder dados; b) Perder negócios porque um desastre destruiu seu prédio e; c) Deixar de cumprir leis e regulamentações. (KIM; SOLOMON, 2014)

Para Kim e Solomon (2014) uma ameaça é qualquer ação que possa danificar um bem. Sistemas de Informação enfrentam ameaças naturais e induzidas por humanos. Ameaças de enchente, terremoto ou fortes tempestades exigem que as organizações tenham planos para garantir que a operação da empresa continue e que a organização possa se recuperar.

Uma vulnerabilidade é um ponto fraco que permita que uma ameaça seja concretizada ou que tenha efeito sobre um bem. Para exemplificar melhor quando o fogo é aceso na churrasqueira ele não impõe perigo, mas o fogo aceso no centro de dados computacionais é muito vulnerável. (KIM; SOLOMON, 2014)

Mas, quem afinal provoca os riscos, ameaças e vulnerabilidade à informação? Para contextualizar o assunto é necessário ter conhecimento dos termos adotados pela área da Tecnologia da Informação. Primeiramente, o entendimento deve começar pelo termo ciberespaço. O termo descreve a rede mundial de computadores – Internet – utilizado por KIM e SOLOMON (2014) surgiu de uma definição adotada pelo FBI –

Federal Bureau of Investigation dos Estados Unidos, no ano de 2002 que atribui o ciberterrorismo como qualquer ataque premeditado e com motivação política contra sistemas de informação, computadores, programas e dados que resultem em violência contra alvos não resistentes realizados por grupos subnacionais ou agentes clandestinos.

É comum a associação ao hacker como agente de ciberterrorismo. Um ciberterrorista é alguém que intimada ou exerce coerção sobre um governo ou uma organização para promover seus objetivos políticos ou sociais, lançando ataques por computador contra outros computadores, redes e informações neles armazenadas. (STAIR; REYNOLDS, 2015).

O crime em informática termo adotado pela AITP – *Association of Information Technology Professionals* retrata uma ameaça crescente para a sociedade, é causada por ações criminosas ou irresponsáveis de indivíduos que estão tirando vantagem do uso abrangente e da vulnerabilidade de computadores, da internet e de outras redes.

Tais crimes são definidos pela AITP como: 1) uso e acesso não autorizados, modificação e destruição de hardware, software, dados ou recursos de rede; 2) liberação não autorizada de informação; 3) cópia não autorizada de software; 4) negar a um usuário final o acesso ao seu próprio hardware, software, dados ou recursos de rede e; 5) usar o computador ou recursos de rede para ilegalmente obter informações ou propriedade tangível. (O'BRIEN; MARAKAS, 2013)

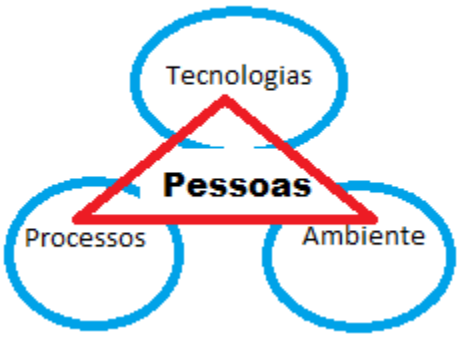
Os ladrões cibernéticos são classificados no ambiente da Internet de várias maneiras. Os atos dos *hackers* que consistem no uso obsessivo de computadores ou acesso e uso não autorizado de sistemas de computadores de redes são executados externamente ou por empregados da empresa que usam a internet e outras redes para furtar ou danificar dados e programas. O termo *hacker* é pejorativamente associado aos ladrões cibernéticos, mas esses *hackers* não promovem furto ou qualquer tipo de dano a pessoas ou empresas. A comunidade da Segurança da Informação diferencia o *hacker* do *cracker*. O hacker são pessoas com conhecimento e habilidade que verificam a vulnerabilidade e as ameaças às empresas ou pessoas através de redes de computadores e equipamentos. Enquanto o *cracker, e*ste sim, uma pessoa com muita habilidade e conhecimento, mas, mal-intencionado e com a finalidade de obter

vantagem financeira sobre as informações que conseguir. (O'BRIEN; MARAKAS, 2013)

De acordo com a pesquisa realizada pela Comptia (2016) nove em cada 10 organizações foram atingidas por pelo menos uma violação (ataque) no ano de 2015. Segundo esse mesmo instituto apenas 13% das empresas brasileiras afirmam não terem sofrido nenhum tipo de violação. Oitenta e um por cento das empresas brasileiras relatam violações de segurança cibernéticas relacionadas a dispositivos móveis, tais como: dispositivos perdidos, *malware* móvel e ataque de *phishing*. Outro ponto alarmante apontado por esse mesmo relatório é que 58% dos riscos a segurança cibernética são por erros humanos contra 42% de erros tecnológicos.

Para Campos (2014) as pessoas também são ativos de informação. Como demostra a Figura 1, são as pessoas que executam os processos e utilizam as tecnologias. Elas geram e consomem as informações nesses processos. São elas que utilizam as tecnologias e os ambientes. É fácil perceber que as pessoas são os ativos mais importantes e, virtualmente podem oferecer os maiores riscos.

Figura 1: Relação entre os ativos de informação



Fonte: O autor adaptado de Campos (2014)

Sabe-se que o objetivo do *hacker* é obter vantagem com informações obtidas de forma ilícita. Para encontrar formas de proteção é necessário identificar os métodos tradicionais de ataques.

2.3 Táticas de Ataques

Segundo O'Brien e Marakas (2013) as principais táticas de ataques dos *hacker* (na verdade, cracker) são:

- Negação de Serviços: Um método comum de ataque que consiste em bombardear na rede o equipamento de um site da web bem com vários pedidos de informação, o ataque pode sobrecarregar efetivamente o sistema, reduzir a velocidade ou até derrubar o site.
- Scans: Consiste em investigar profundamente na internet para determinar os tipos de computadores, serviços e conexões em uso. Desta forma, os "bandidos" podem tirar proveito da fraqueza em determinado software ou recurso de um computador.
- Farejadores: Programas que ocultamente pesquisam pacotes individuais de dados quando passam pela internet, capturando senhas ou conteúdos inteiros.
- Spoofing: Falsificar endereço de e-mail ou página web para ludibriar os usuários para passar adiante informações importantes, como senha e dados do cartão de crédito.
- Cavalo de Tróia: Um programa desconhecido ao usuário, que contém instruções que exploram uma vulnerabilidade conhecida de algum software.
- Back Doors: Quando a porta de entrada é descoberta, usam caminhos ocultos de apoio para tornar a reentrada fácil – e difícil de detectar. (Porta é o meio pelo qual a comunicação de um dispositivo a outro é realizado pela internet)
- Applets nocivos: programas muito pequenos que abusam dos recursos do seu computador, modificam arquivos no disco rígido, enviam e-mail falso ou roubam senhas.
- Password Crackers: Software que consegue descobrir senhas.

- *Adware:* é um software que enquanto diz servir para alguma função útil, e geralmente executando aquela função, também permite aos anunciantes da internet mostrar seus anúncios por meio de banners e *pop-ups* sem o consentimento do usuário. Ele também pode coletar informações sobre o usuário do computador e mandar via internet para o seu desenvolvedor. Por esta razão também são conhecidos como *spyware*. Neste caso, coletam informações específicas sobre o usuário como: nome, endereço, telefone, hábitos, senhas e, se possível, dados de cartão de crédito.
- Engenharia Social: Uma tática usada para obter acesso a sistemas de computadores conversando insuspeitamente com quem deseja obter informações valiosas, como senhas. A ação pode ser praticada em um funcionário de uma empresa ou até mesmo um usuário convencional.

2.4 Mecanismos de Prevenção

Ferreira (2003) prioriza a prevenção em métodos que devem ser iniciados pelo principal mecanismo de acesso às informações: as pessoas. Neste caso, esses mecanismos devem ter algumas características básicas. Os sistemas devem ser capazes de registrar o acesso das pessoas, mas, sobretudo que permita consulta posteriores (para monitoria e auditoria). Em acessos válidos gravar data, hora, local e identificação da pessoa.

A autenticação por senha é importante e traz garantias adicionais a permissão de acesso aos sistemas que não deve ser desprezada. Uma senha deve ser forte o suficiente para não comprometer o sistema, mas não deve ser fácil para que todos possam ter acesso. Por exemplo, a data de nascimento, ou sequencias numéricas. Por outro lado, não pode ser extremamente complexa que para memoriza-la o usuário precise anotá-la e deixar a anotação em um pedaço de papel sobre a mesa de trabalho.

Em situações onde a segurança deve ser reforçada a utilização de segurança biométrica não pode ser descartada. Os dispositivos de controle biométrico usam sensores que avaliam características físicas que tornam cada indivíduo único. Inclui

verificação de voz, digitais, geometria da mão, dinâmica da assinatura, análise de digitação, varredura de retina, reconhecimento da face e análise do padrão genético.

As medidas essenciais para prover segurança a sistemas e informações que estão em servidores, computadores e demais dispositivos deve começar com a adoção de antivírus. Os antivírus são softwares que tem o objetivo de proteger os equipamentos contra vírus, *worms*, cavalos de Tróia e outros programas nocivos. (O'BRIEN; MARAKAS, 2013)

Em segundo lugar, usar códigos de segurança (senhas) fortes. Essas senhas são reconhecidas como menos suscetíveis a ataques quando constituídas por letras, números e símbolos. Tendo pelo menos, uma letra maiúscula. Além disso, a frequente mudança de senhas garante um nível de segurança melhor aos usuários.

Procedimentos de cópia de dados (backup) devem ser realizados com a frequência exigida pela importância da informação. Sendo a informação um ativo valioso para a organização e para as pessoas a falta dele pode trazer prejuízos irreparáveis. (O'BRIEN; MARAKAS, 2013) Equipamentos sobressalentes devem ser disponibilizados e colocados em uso no menor período de tempo possível, depois de paralisado o sistema de controle principal. Independente da forma adotada o importante e manter o sistema atualizado com as mesmas características sem modificações em razão da utilização de um procedimento de backup. (FERREIRA, 2003)

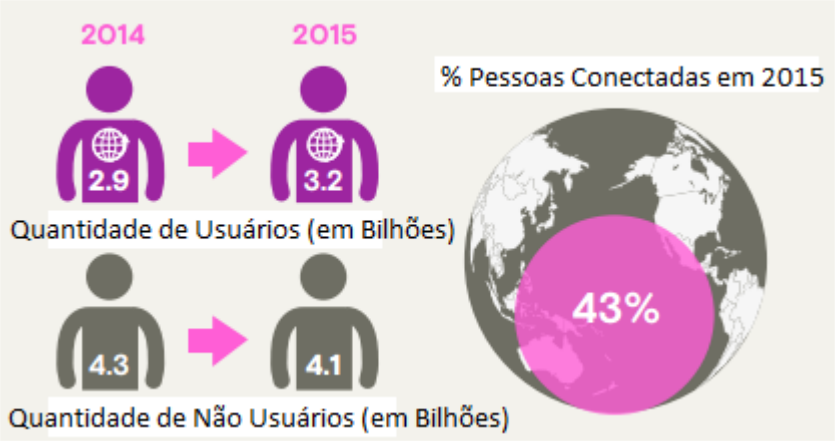
Os ataques de Negação de Serviço (DoS) podem ser minimizados com reforço na política de segurança. Verificando regularmente – através de programas (softwares) a existência nos servidores de programas do tipo cavalo de Troia, e gerenciamento o aumento inesperado no tráfego da internet.

Outro importante método de controle e segurança na internet e outras redes é o uso de computador e software de firewall. Um firewall trabalha como um sistema de "porteiro" protegendo as intranets e outras redes de computadores da empresa de invasões, fornecendo um filtro e um ponto de transferência seguro para acessar a internet. (O'BRIEN; MARAKAS, 2013)

3 Resultados e Discussões

Com o objetivo de identificar o estado da conectividade mundial o Facebook financia através do Instituto Internet.org pesquisas para nortear projetos e facilitar o acesso à informação em toda parte do mundo. No relatório de conectividade do ano de 2015 e, apresentado na Figura 2, destaca o aumento de usuários da Internet e a diminuição de pessoas que não estavam conectadas e aderiram ao mundo virtual. (INTERNET.ORG, 2016)

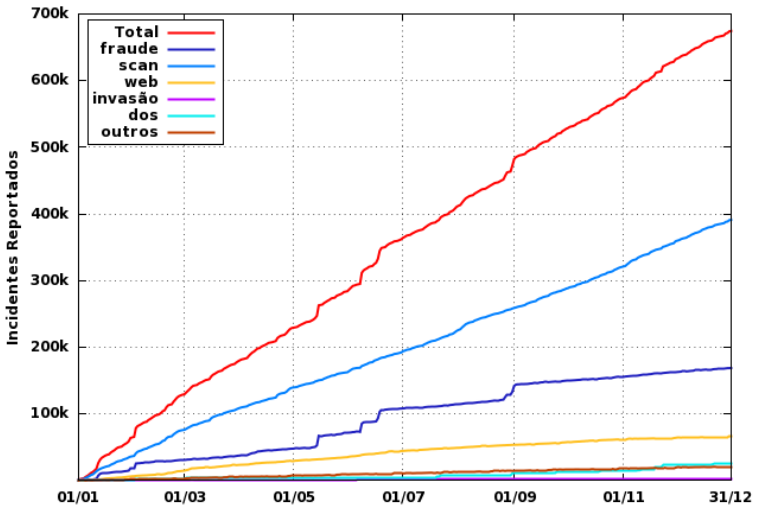
Figura 2: Evolução de usuários da Internet



Fonte: O Autor adaptado de Internet.Org (2016)

Nota-se através do Gráfico 1, disponibilizado pela Cert (2016) que houve um aumento considerável dos incidentes no ano de 2015 em todos os itens mencionados como principais táticas de ataque. O Instituto concentra alguns itens na modalidade fraude como os Applets nocivos e Password Crackers, cujo objetivo é a obtenção de dados dos usuários especialmente senhas. A incidência total no decorrer do ano de 2015 atingiu a marca superior a 650 mil ataques. Essa incidência está relacionada, indiscutivelmente, ao aumento de usuários das redes, sobretudo a internet e, a pouca importância à segurança das informações.

Gráfico 2: Incidentes Reportados no ano de 2015



Fonte: CERT (2016)

Como a informação é um ativo essencial para os negócios de uma organização ela deve ser adequadamente protegida. Como um resultado deste incrível aumento de interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. (ABNT, 2005)

Por esta razão, todos os usuários devem proteger as suas informações adotando mecanismos essenciais como antivírus e firewall em computadores pessoais. E, no caso de organizações softwares de controle de acesso, gerenciamento de rede e firewall para servidores. Com a adoção de medidas simples consegue-se mitigar uma grande quantidade de ameaças como as relatadas anteriormente.

4 Conclusões

É inegável que as informações são de extrema importância para pessoas, empresas e governo. Indiscutivelmente, o acesso a essas informações, na atualidade, está a cada dia mais fácil e ágil. Infelizmente, a facilidade que se tem acesso às informações não corresponde às preocupações com medidas de prevenção. A cada dia, novas formas de tecnologia estão sendo utilizadas, tudo começou com as páginas

da internet, hoje, temos vídeos, mensagens de voz e animações na mesma tecnologia. Mas, por outro lado, com a mesma rapidez que as novidades tecnologias estão sendo disponibilizadas, novas técnicas de ataque também os são. Conhecer as técnicas de ataque e os objetivos desses cibercriminosos é fundamental para garantir a prevenção. Em Segurança da Informação não se pode garantir que ataques não acontecerão, mas as proteções e barreiras de segurança devem ser utilizadas de todas as formas. As ameaças estão por toda parte. Não se deve acreditar apenas na tecnologia quando o principal ativo da informação são pessoas que protelam mecanismos de segurança acreditando que nada acontecerá porque as suas informações não são valiosas. Pelo contrário, o hacker não faz distinção de pessoas, ela ataca aquele que está mais vulnerável. Desta forma, este Artigo contribui para divulgar e alertar os usuários sobre a necessidade de adoção de mecanismos de segurança. Os principais incidentes de segurança foram apresentados e, soluções simples que permitem garantir a proteção da informação também foram expostos. A Segurança da Informação é complexa e cheia de nuances, mas medidas básicas de prevenção possibilitarão garantias e tranquilidade para navegar neste universo tão interessante denominado Internet.

Referências

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

BRASILEIRO, A. M. M. **Manual de produção de textos acadêmicos e científicos**. São Paulo: Atlas, 2013.

CAMPOS. A. **Sistema de segurança da informação: controlando os riscos.** 3. ed. Florianópolis: Visual Books, 2014.

CERT - CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Tipos de Ataques Reportados ao CERT.BR**. Disponível em: < http://www.cert.br/stats/incidentes/2015-jan-dec/tipos-ataque-acumulado.html> Acesso em: 06 set 2016.

COMPTIA. **Full Report CompTIA 2016 channel security vfinal.** Disponível em <https://www.comptia.org/resources/security-in-the-it-channel?c=34300> Acesso em: 26 ago. 2016.

FERREIRA, F. N. F. **Segurança da Informação**. Rio de Janeiro: Editora Ciência Moderna, 2003.

INTERNET.ORG. **A Report on Global Internet Access.** Disponível em <https://fbnewsroomus.files.wordpress.com/2016/02/state-of-connectivity-2015-2016-02-21-final.pdf> Acesso em: 06 out 2016.

KIM, D.; SOLOMON, M. G. **Fundamentos de segurança em sistemas de informação**. Tradução Daniel Vieira; Rio de Janeiro: LTC, 2014.

O'BRIEN, J. A; MARAKAS, G. M. **Administração de Sistemas de Informação**. Tradução Rodrigo Dubal; revisão técnica: Armando Dal Colleto. – 15. ed. Porto Alegre: AMGH, 2013

PONTES, E. **Políticas e normas para segurança da informação** Rio de Janeiro: Brasport, 2012.

STAIR, R. M; REYNOLDS, G. W. **Princípios de Sistemas de Informação**. Tradução Noveritis do Brasil. 11. ed. São Paulo: Cengage Learning, 2015.

WORLD BANK. World Bank Group. **World Development Report 2016 APP**. Disponível em <http://www.worldbank.org/en/publication/wdr2016> Acesso em 25 ago. de 2016