SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DA INTERNET COM ÊNFASE EM CERTIFICAÇÃO DIGITAL

BERNARDINELLI, Mário César Reato – mariocrb@yahoo.com.br
GONÇALVES JUNIOR, Nelson (Orientador) – nelsongjr@gmail.com

RESUMO

A tecnologia da informação vem passando por um processo de evolução muito rápido e torna a vida de seus adeptos e usuários cada vez mais acessível, interativa, funcional e com possibilidades ilimitadas através principalmente das redes de computadores que estão distribuídas por todo o mundo, na qual, a internet vem alavancando esse processo, porém, com ela a necessidade de garantir a segurança da informação com intuito de salvaguardar e manter o sigilo de informações confidenciais ou até mesmo identificar computadores, pessoas e diversos dispositivos, para então, disponibilizar acesso a estes de conteúdos e serviços diferenciados e restritos. A Certificação digital é uma solução para o problema de segurança da informação em redes públicas e privadas, no qual, permite uma maior garantia de confidencialidade, autenticidade, integridade, disponibilidade e controle de acesso no ambiente virtual, porém, é necessário conciliar outros recursos com ela para obter-se um melhor resultado, como análises de ameaças, politicas de seguranças e outras ferramentas que visem minimizar o problema que envolve a segurança e dificultar as perdas de informações.

Palavras Chaves: Redes, Segurança, Informação e Certificação Digital.

ABSTRACT

Information technology is undergoing a very fast process of evolution and making the lives of its users increasingly accessible, interactive, functional and with unlimited possibilities specially through computer networks that are distributed throughout the world, in which the Internet is helping this process to happen, but with it the need to ensure information security in order to safeguard and maintain the confidentiality of confidential information or even identify computers, people and various devices to provide then access to this content and differentiated services and restricts. The Digital Certification is a solution to the problem of information security in public and private networks, which allows greater assurance of confidentiality, authenticity, integrity, availability and access control in virtual environment, however, it is necessary to reconcile it with other resources to obtain a better result, as analysis of threats, security policies and other tools that aim to minimize the problem involving the safety and hinder the loss of information.

Keywords: Networks, Security, Information and Digital Certification.

INTRODUÇÃO

A informática vem avançando gradativamente e torna-se cada vez mais comum o relacionamento entre pessoas, computadores, equipamentos e outros através da rede de computadores e principalmente na internet, onde milhões e milhões de pessoas trocam informações pelo mundo todo dia, seja a trabalho, interatividade, pesquisas e muito mais tornando cada vez mais evidente a necessidade de proteger e garantir a integridade e segurança de parte desse conteúdo através de uma ferramenta que possibilite a confidencialidade e direito de propriedade da informação e atualmente uma das melhores ferramentas para isso é conhecida como “Certificação Digital”.

As redes de computadores consistem em no mínimo dois ou mais computadores conectados com a finalidade de compartilhar dados, informações, serviços, recursos e outras. Entretanto é necessário observar os principais critérios para a segurança dessa rede, dentre esses, destacam-se os seguintes: a confidencialidade, a autenticação, a integridade e a disponibilidade ou controle de acesso, visando garantir a integridade e segurança da informação e salvaguardando os direitos de propriedade do detentor da mesma. E uma forma de garantir a segurança é através da criptografia que embaralha a informação buscando ocultar seu significado de maneira que somente quem possui sua estrutura pode decifrar o mesmo, e uma ferramenta essencial é a certificação digital que permite garantir à integridade e segurança da informação proporcionado a identificação de pessoas, empresas, computadores, aplicações e outras que possam existir de maneira eletrônica.

Na utilização da certificação digital faz-se necessário seguir algumas exigências e cuidados com segurança, na qual, as grandes e médias organizações possuem regulamentos e práticas que especificam bem quais os cuidados a serem tomados, porém, em algumas pequenas organizações ou usuários comuns não tem esse tipo cuidado e não dão o devido valor ao armazenamento adequado e a usabilidade do certificado digital, ocasionado muitos problemas, prejuízos e perdas relativas ao mesmo.

SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DA INTERNET COM ÊNFASE EM CERTIFICAÇÃO DIGITAL

Uma rede de computadores pode ser entendida como no mínimo dois ou mais computadores conectados com a finalidade de compartilhar dados, informações, serviços, recursos e outras. Agora imagine um ambiente onde se tem milhões e milhões de computadores, dispositivos entre outros que possibilitam as pessoas a interagirem e compartilharem informações entre si, esta pode ser chamada de internet. Em função dessa infinidade de possibilidades faz necessário tornar a rede um ambiente mais seguro que possibilite: confidencialidade (tem como objetivo proporcionar acesso da informação somente a quem tiver permissão); autenticação (atesta a autenticidade da informação visando garantir a identidade de quem encaminhou à respectiva); integridade e não-repudiação de mensagem (visa proporcionar uma informação confiável e segura durante o processo de sua transmissão); e disponibilidade e controle de acesso (dispõem sobre a acessibilidade proporcionando funcionamento contínuo com um bom desempenho).

A segurança da informação visa garantir ao responsável que detém a respectiva de inúmeros tipos de ameaças e ataques visando garantir a confidencialidade e integridade da informação proporcionando segurança, maximização da riqueza, domínio de tecnologia e muitos outros, isto é, informações com grande valor agregado pode determinar a vantagem competitiva em um determinado ramo de atividade, setor, mercado de atuação e outros de forma a se tornar um diferencial que pode determinar o sucesso ou fracasso de uma organização. E uma das maneiras mais eficientes é através da criptografia que é o estudo de uma informação embaralhada buscando ocultar significado de maneira que somente quem possui sua estrutura possa decifrar o mesmo, e também, através de uma política de segurança da informação bem elaborada, delimitando o ponto de atuação e as maneiras como devem ser executados alguns métodos e serviços de forma a padronizar e mensurar possíveis problemas futuros. Porém, é difícil garantir que somente quem possui a solução pode decifra-la e que não haja formas de burlar a política de segurança.

Certificação digital é uma das tecnologias de segurança da informação mais utilizadas, isto é, uma ferramenta essencial surgida em função da necessidade de

manter a integridade e segurança da informação, bem como, alimentar o sistema público, permitir uma melhor segurança na interação junto à internet, em fim, assegurar todas as relações eletrônicas. Ela beneficia diversas áreas e setores de nossa economia proporcionando uma melhor segurança e integridade da informação, dentre elas: acompanhamento de processos jurídicos online; entrega de obrigações principais e acessórias de maneira simplificada e segura; maior segurança na web; e muitas outras. Através da certificação digital é possível gerar um certificado digital, que podem ser entendido como um documento digital que visa identificar pessoas, empresas, computadores, aplicações e outras que possam existir de maneira eletrônica, dentre esses vale destacar: e-CPF (certificado digital pessoa física) e o e-CNPJ (certificado digital pessoa jurídica). Porém, todos eles apresentam uma estrutura semelhante e possuem os seguintes campos: versão (número da versão), número de série (identificador único do certificado), algoritmo de assinatura (semântica e lógica), emissor (autoridade certificadora), período de validade (duração do certificado), assunto (dono da chave pública do certificado), chave pública (informações e algoritmos com a qual a chave deve ser usada), extensões (campo para adição de informações complementares).

Os certificados digitais gerados possuem um repositório onde se obtém informações referentes aos certificados digitais chamada de lista de certificados revogados, no caso do Brasil, a Autoridade Certificadora da ICP – Brasil utiliza o modelo básico. No entanto, existem diversos outros tipos de listas e dependendo do crescimento da lista a tendência será a implantação de novos modelos de lista a fim de evitar gargalos na requisição no repositório, tornando o processo mais rápido e eficiente.

Atualmente, em função, do aumento da utilização da ferramenta certificação digital através dos certificados digitais faz-se necessário seguir algumas exigências e tomar alguns cuidados com a segurança do mesmo, tais como: as Autoridades Certificadoras tem de observar a Declaração de Práticas de Certificação, Políticas de Certificado, Políticas de Segurança e outras estabelecidas pela Autoridade Certificadora Raiz, já as grandes e médias organizações possuem regulamentos e práticas próprias estabelecidas pela auditoria que especificam bem quais os cuidados a serem tomados e como seus funcionários devem se comportar quando

ao seu manuseio, porém, em algumas pequenas organizações ou usuários comuns não tem esse tipo de cuidado, até mesmo, às vezes por ter um ambiente familiar, para tanto, citamos algumas das práticas de segurança mais comuns a todos aos usuários que podem evitar problemas relacionados com o certificado digital, tais como: somente o titular da chave privada deve manusear e utilizar o certificado digital; não compartilhar a senha do certificado digital com ninguém; caso a chave criptográfica possua materialidade guardar em local apropriado que somente o titular do cartão tenha acesso. Muitos desses usuários de certificado digital não dão as devidas importâncias ao armazenamento adequado e usabilidade do mesmo, ocasionado muitos prejuízos, pois, não entendem que uma assinatura digital corresponde a uma assinatura com reconhecimento de firma e acabam descobrindo quando já é tarde demais ou quando terceiros se aproveitam e o usam indevidamente. Portanto, é necessário manter seu certificado digital em local seguro e adotar algumas práticas e procedimentos de segurança que visem melhorar, selecionar, manusear de maneira mais adequada o respectivo.

RESULTADOS E/OU DISCUSSÃO

A certificação digital é um assunto muito abrangente e pode ter uma infinidade de aplicações seja para realizar criptografias com intuito de proteger informações quanto a disponibilização de serviços junto ao meio público como por exemplo: acesso aos portais eletrônicos que permitem que o usuário do certificado resolva uma infinidade de situações com apenas alguns cliques sem precisar sair de sua residência ou organização evitando filas e transtornos que ocorrem no dia a dia, além dessas existem outras possibilidades que podem ser aplicadas de acordo com a necessidade do usuário.

Atualmente existe uma grande perspectiva quanto a implantação do certificado digital para toda a população brasileira prometendo unificar diversos documentos de uso pessoal em apenas um único chamado de “Registro Único de Identidade Civil” e possivelmente com a implantação desse sistema surgirá novas formas e aplicações para o mesmo.

CONSIDERAÇÕES FINAIS

Redes de computadores tem a finalidade de possibilitar o relacionamento e interação a fim de facilitar o acesso à informação seja numa rede privada ou pública, isto é, visa o compartilhamento de informação entre dispositivos, computadores, pessoas entre outros que se relacionam entre si. Atualmente, está muito difundido principalmente o uso da internet que permite o acesso a um ilimitado conteúdo, a maior parte destes na figura de pessoas que já utilizaram ou utilizam direta ou indiretamente as diversas possibilidades disponibilizadas por esse meio de comunicação inovador que tende a cada vez mais se tornar acessível, interativo, funcional e ilimitado.

Segurança é um assunto que preocupa a todos em todas as esferas públicas ou privadas no Brasil, e neste caso, com o ambiente virtual não é diferente, pois, faz-se necessário tomar precauções para não perder informações cruciais e importantes que possam possibilitar a terceiros: vantagens competitivas, financeiras, gerenciais e muitas outras. Na era digital a informação pode valer ouro e nas mãos erradas podem ser utilizadas de forma errada e causar grandes prejuízos a organizações, entidades, pessoas e a todos que dependem dela. Por isso, é essencial utilizar a tecnologia a nosso favor a fim de tornar o ambiente virtual protegido e um lugar mais seguro, no qual, as partes possam utiliza-la para desempenhar suas atividades e processos sem medo de ocorrer perdas e prejuízos sejam eles financeiros, tecnológicos, morais entre outros.

Certificação Digital atualmente é uma das principais ferramentas utilizadas para garantir a segurança, integridade, identidade da informação envolvida. Ela possibilita diversas formas concretas para isso, o mundo se torna cada vez mais digital e com ele a necessidade de saber o que é real ou não, quem é quem e muito mais. Por isso, uma das formas mais lógicas para obter-se: confidencialidade, autenticidade, integridade, disponibilidade e controle de acesso nas redes de computadores por todo o mundo e principalmente garantir as partes que participam deste é a certificação digital, mais somente isso não resolve, é necessário junto com ela estabelecer politicas de segurança da informação, criptografias, análises de

ameaças e muito mais visando minimizar este problema de segurança e dificultar ao máximo a perda de informações.

REFERÊNCIAS BIBLIOGRÁFICAS

AQUINO JUNIOR, IVANILDO JOSÉ DE SOUZA; BATISTA, EDUARDO MAZZA; HOMOLKA, HEBERT OTTO; LIMA, MARCELO FERREIRA DE; SILVA, LUIZ GUSTAVO CORDEIRO DA. E SILVA, PAULO EDUARDO DA. **Certificação Digital - Conceitos e Aplicações - Modelos Brasileiro e Australiano**. 1ª ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

CERTISIGN. Disponível em http://www.certisign.com.br/. Acesso em: 07 de junho de 2010 às 10:54.

ITI – Instituto Nacional da Tecnologia da Informação. Disponível em http://www.iti.gov.br/. Acesso em: 24 de agosto de 2010 às 08:29.

KUROSE, JAMES F e ROSS, KEITH W. **Redes de Computadores e a Internet**. 3ª ed. São Paulo: Editora Pearson Addison Wesley, 2006.

MENEZES, JOSUÉ DAS CHAGAS. **Gestão da Segurança da Informação**. 1ª ed. Campinas: Editora J. H. Mizuno, 2006.

MORAES, Anna Maris Pereira. **Iniciação ao Estudo da Administração**. 2ª Ed. São Paulo: Makron Books, 2000.

RECEITA FEDERAL DO BRASIL. Disponível em http://www.receita.fazenda.gov.br. Acesso em 25 de agosto de 2010 às 10:45.

SERASA EXPERIAN. Disponível em http://www.certificadodigital.com.br. Acesso em 07 de junho de 2010 às 11:04.

SOARES, Luiz Fernando Gomes; LEMOS, Guido e COLCHER, Sérgio. **Redes de Computadores**. 2ª ed. Rio de Janeiro: Editora Campus, 1995.

TANEMBAUM, ANDREW S. **Redes de Computadores**. 3ª ed. Rio de Janeiro: Editora Campus, 1997.