Developers' Magazine On-Line
http://www.developers.com.br

Edição 83, Julho de 2003.

Aspectos de Privacidade e Segurança em Extranets Coorporativas

Rodrigo Felicio dos Santos & Francisco Gomes Milagres

Com o objetivo de facilitar o acesso à informação e a transparência de todos os níveis do processo de negócio, as corporações estão estudando novas formas de acesso às suas infra-estruturas computacionais. Assim, possibilitam aos seus clientes e parceiros o acesso a suas chamadas *extranets*. O conceito usado para exteriorizar os setores corporativos permite, por exemplo, uma aproximação do cliente ao negócio da empresa e também uma redução de investimentos em estruturas físicas como no caso de um modelo de *Internet Banking*.

Paralelamente, são cada vez mais perceptíveis em publicações especializadas as características de novos processos e ferramentas que visam garantir a segurança de sistemas desta natureza. Para que seja possível afirmar que a segurança de um sistema ao menos é mantida em níveis aceitáveis (obter um nível máximo de segurança não é algo prático ou factível) devem ser garantidos, entre outros fatores, a privacidade do usuário, o sigilo e a integridade das informações, além da disponibilidade e o controle de acesso.

O objetivo deste artigo é apresentar algumas das vulnerabilidades que surgiram com este modelo de abertura de negócios através da Internet e também mostrar algumas soluções que permitem aumentar o nível mínimo de segurança para garantir a continuidade de negócios através da rede mundial.

Segurança em Comunicação de Dados

Para garantir a segurança em ambientes que requerem a comunicação de dados como, por exemplo, em *extranets*, devem ser consideradas as suas três principais componentes: o servidor corporativo, o canal de comunicação e a aplicação cliente.

Geralmente, servidores corporativos são compostos de servidores para páginas web e com acesso restrito a bancos de dados corporativos como, por exemplo, portais de empresas que centralizam a disponibilização de informações para colaboradores, parceiros e clientes. O canal de comunicação, na maioria das empresas utiliza como base a Internet, o que possibilita o acesso às informações da empresa de qualquer parte do planeta usando diferentes formas de acesso (por exemplo, linhas discadas, redes rápidas e dedicadas ou sem fio). A componente final da tríplice de acesso à informação corporativa neste modelo de *extranet* é a aplicação cliente de navegação web, como os navegadores Netscape, Mozilla ou Internet Explorer.

Segurança no Processo Cliente/Empresa

Para garantir a segurança na comunicação de dados, inicialmente devem ser consideradas, entre outras diretrizes, as políticas de segurança e de privacidade de cada parte envolvida na comunicação. Sendo assim, será analisado cada componente deste processo, ou seja, o cliente, o canal de comunicação e a empresa responsável pelo serviço oferecido devem prosseguir para que haja um nível mínimo de segurança na troca de informações entre ambas as partes.

Cliente: alguns cuidados básicos podem ser tomados para que a privacidade do usuário e a integridade da informação sejam mantidas. Evitar o uso de quiosques públicos como *cyber cafés* é uma medida de prevenção simples, já que ao utilizarmos estes estabelecimentos, podemos deixar a janela do *browser* aberta. Caso esta ação venha a ocorrer, outros usuários terão acesso às informações deixadas pelo usuário anterior no browser, o que não é nada conveniente.

Algumas propriedades do *browser* também podem ser desabilitadas para que o armazenamento de informações restritas, como senhas e dados pessoais, não possa ser efetuado no computador do cliente, protegendo-o assim de um eventual acesso indevido de usuários não-autorizados.

A propriedade auto-completar de *browsers* como Netscape e Internet Explorer, por exemplo, já vem habilitada. Esta propriedade é responsável pelo preenchimento automático de formulários eletrônicos incluindo campos para inserção de senha, e endereços web. No entanto, esta característica possui pontos positivos e negativos que devem ser considerados. Ao auto-completar endereços web no Internet Explorer, por exemplo, a economia de tempo pode ser explícitamente notada, em especial se não nos recordamos do endereço exato do site que visitamos dois dias atrás. No entanto, torna-se fácil o uso dessa informação por pessoas mal intencionadas que tenham interesse em descobrir quais sites foram visitados. Dessa forma é possível traçar um perfil do usuário e bombardeá-lo com ofertas de produtos de sua preferência.

Embora a praticidade e economia de tempo desta propriedade sejam características realmente atrativas, em alguns sites como bancos virtuais, há a necessidade desta propriedade ser desabilitada. Desse modo, o usuário estaria mais protegido contra o roubo de informações sigilosas como números de cartões de crédito, etc.

Canal de Comunicação: considerando-se a Internet como meio para realização de troca de informação entre cliente e empresa, são utilizados protocolos responsáveis por

codificar e autenticar a informação fornecida por ambas as extremidades do canal: o cliente e a empresa. Para isso, alguns protocolos podem ser utilizados, entre eles o SSL – *Secure Sockets Layer* e o TLS – *Transport Layer Security*, os quais são responsáveis pela privacidade da informação que trafega através da Internet.

Ambos possuem duas características principais: algoritmos de codificação, os quais permitem codificar/decodificar os dados ao longo do processo, e certificados digitais, que fornecem a autenticação tanto do cliente quanto da empresa provedora do serviço. Os algoritmos de codificação ou criptografia são classificados como simétricos ou assimétricos.

Os simétricos utilizam uma única chave, usada tanto para codificar quanto para decodificar os dados. Portanto, os dados codificados estão seguros somente se a chave pode ser distribuída de modo confiável a ambas as partes. Em algoritmos assimétricos há um par de chaves, uma pública e outra privada. A chave pública tem a função de codificar os dados, embora não possa ser usada para decodificá-los. Este dever recai sobre a chave privada. Portanto, as informações codificadas com a chave pública podem ser consideradas seguras se a chave privada estiver segura. Outro fator importante a ser considerado é o tamanho das chaves usadas. Chaves simétricas de 40 ou 56 bits são chaves teoricamente fáceis de serem quebradas, enquanto que as de 128 bits são mais robustas e, matematicamente, mais difíceis de serem decifradas. O uso de chaves assimétricas em comunicações seguras nos *browsers* Internet geralmente se dá no estabelecimento da conexão, ou seja, quando há necessidade de troca da chave simétrica para comunicação.

Os certificados digitais podem ser usados por clientes e empresas e permitem a autenticação das duas partes envolvidas na transação. Logo, são assegurados pelas chamadas Autoridades de Certificação (AC), como a Certisign, por exemplo, as quais atuam como uma entidade externa do processo e que por natureza deve ser confiável. Dentro do certificado estão informações como número serial, o nome da AC, a validade do certificado, uma chave pública e a assinatura digital da AC.

Empresa: além do uso de protocolos como SSL e TLS, as empresas podem tomar medidas para fornecer cada vez mais segurança e confiabilidade por meio de medidas simples na criação de portais. Em *Internet Banks*, por exemplo, muitos bancos estão aderindo ao uso de teclados virtuais em seus portais, apesar de recentes alertas já notificarem a existência de aplicativos hostis que capturam posições e cliques do mouse. Outro exemplo é a possibilidade de desabilitar a opção auto-completar dos navegadores para que informações sigilosas como senhas não sejam acessadas por pessoas não autorizadas. Para isso, basta apenas acrescentar o atributo *auto-complete=”off”* na tag HTML do formulário.

Artifícios mais robustos e sofisticados também são soluções válidas. É o caso de plataformas como o P3P – *Platform for Privacy Preferences Project*, do W3C (*World Wide Web Consortium*), um padrão que permite uma forma simples e automatizada de garantir aos usuários o controle de privacidade dos sites que visitam. Constituído basicamente de um conjunto de perguntas e respostas que abrangem todos os aspectos da política de privacidade do site, o P3P permite que cada cliente tenha informações de como seus dados pessoais são utilizados pelos sites que seguem uma política definida de privacidade. Por utilizar um padrão aberto e compreensível tanto pelos usuários como

pelas aplicações, há certamente um aumento do nível de confiança para qualquer serviço prestado por este.

Recomendações de Segurança

O passo inicial para a definição dos processos e ferramentas que visam garantir a segurança da informação é a definição dos riscos que uma empresa e seus ativos correm e o estabelecimento de políticas de uso, segurança e privacidade, por exemplo. Com a necessidade de abertura cada vez maior do contato das empresas com seus colaboradores, a Internet tem sido a principal escolha como meio de comunicação, apesar de ser um ambiente geralmente hostil quando são ponderados os prós e contras em segurança.

Considerando recomendações mínimas de segurança nas partes envolvidas, neste caso, nas empresas e nos seus clientes, é possível obter bons níveis de garantia de segurança, privacidade e continuidade dos negócios. Do lado das empresas, a responsabilidade recai principalmente por mostrar com transparência os processos utilizados para garantí-la. Por outro lado, os clientes devem utilizar os recursos de proteção disponibilizados pelas ferramentas em questão, os navegadores Internet, além de ferramentas adicionais para segurança de e-mails e na conexão à Internet.

Rodrigo Felício dos Santos `<felicio @ icmc.usp.br>` é Mestrando em Ciências da Computação pelo Instituto de Ciências Matemáticas e de Computação (ICMC) da Universidade de São Paulo (USP), em São Carlos, nas áreas de computação ubíqua, transmissão de vídeo e redes sem fio. Atua há um ano e meio como pesquisador do Grupo de Multimídia no Laboratório Intermídia em consciência de contexto.

Francisco Gomes Milagres `<milagres @ icmc.usp.br>` é Mestrando em Ciências da Computação pelo Instituto de Ciências Matemáticas e de Computação (ICMC) da Universidade de São Paulo (USP), em São Carlos, nas áreas de segurança em redes sem fio e computação ubíqua. Atua há quatro anos como pesquisador do Grupo de Segurança Computacional no Laboratório Intermídia em atividades de Pesquisa e Extensão em Segurança da Informação, é consultor em projetos de segurança da informação em organizações do estado de São Paulo e também editor do portal Milagres.com, onde apresenta suas pesquisas e publicações em veículos especializados nacionais e internacionais.

Links:

How to Turn Off Form Autocompletion
http://devedge.netscape.com/viewsource/2003/form-autocompletion/

Platform for Privacy Preferences (P3P) Project
http://www.w3.org/P3P/

Disable AutoComplete for forms
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/723.asp

Do not allow AutoComplete to save passwords
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gp/724.asp

Transport Layer Security (TLS)
http://www.ietf.org/html.charters/tls-charter.html

Secure Sockets Layer (SSL)
http://wp.netscape.com/eng/ssl3/

Certisign
http://www.certisign.com.br