ABORDAGEM DE SISTEMAS DE INFORMAÇÃO ENFOCANDO A SEGURANÇA EM AMBIENTES INTERNET/INTRANET/EXTRANET

Fábio Câmara Araújo de Carvalho, Mestrando
Cristiano Hugo Cagnin, Mestrando
Aline França de Abreu, PhD
João Ernesto Escosteguy Castro, M. Eng.

UFSC/CTC/EPS, Caixa Postal 476 – CEP-88040-900 - Florianópolis/SC – IGTI – Núcleo de Estudos em Informação, Gestão e Tecnologia da Informação & LabSAD – Laboratório de Sistemas de Apoio à Decisão – fbcamara@eps.ufsc.br, cagnin@eps.ufsc.br, aline@eps.ufsc.br, castro@eps.ufsc.br

Área temática: Estratégia, Organizações e Tecnologia

ABSTRACT: In the present configuration of business, characterized by globalization, production processes' automation and fast technological evolution (including hardware, software and telecommunications), the enterprises are searching for new market by trying to adapt their information systems to capture, treat, distribute, dissipate and exchange information in the internet/intranet/extranet environment, in order to obtain higher effectiveness and to share their knowledge with their employees. These changes lead to the valorization of human resources and information as strategic resources for the organizations to promote competitive advantage and to guarantee their survival. Information systems and the users' attitude towards them, as well as the new computational tools for decision making and information resource management, became critical factors to obtain competitiveness. Therefore, the security of the information inside the data bases (data warehouses) or inside the management information systems becomes a very important strategy among others to maintain their wealth and their competitive advantage, since they are based on information and knowledge. But to ensure this scenario it is necessary a behavioral change from everybody engaged in the business process. Then, this paper discusses the use of the most updated technology which supports the new concept of business information architecture and the security issue in the internet/intranet/extranet environment, as well as, the behavioral changes necessary to achieve competitiveness.

KEYWORDS: information systems, information security, internet/intranet/extranet environment

RESUMO: No atual cenário mundial dos negócios, caracterizado pela globalização, a automação dos processos produtivos e a rápida evolução tecnológica (abrangendo hardware, software e telecomunicações), as empresas vêm buscando novos mercados através da adaptação de seus sistemas de informação para captação, tratamento, distribuição, disseminação e troca de informação no ambiente *internet/intranet/extranet*, no sentido de obter maior efetividade e também para compartilhar o conhecimento entre todos os que participam do processo de dinamizar o negócio, ou seja, o capital humano da empresa. Estas mudanças convergem para a valorização do ser humano e da informação, ocasionando o aparecimento de organizações baseadas na informação e no conhecimento como bens estratégicos que garantam sua vantagem competitiva e sua sobrevivência. Assim, a segurança das informações contidas em bases de dados (*data warehouses*) ou em sistemas de informações gerenciais passa a ser fundamental para que a empresa mantenha a posse de seus maiores bens: a informação e o conhecimento. O presente artigo pretende mostrar o que há no momento em termos de tecnologia e arquitetura de informação para suporte aos usuários de sistemas das organizações, apresentar a problemática da segurança da informação nos ambientes *internet/intranet/extranet* e mostrar a necessidade da mudança comportamental de todos que participam do processo do negócio da organização como fatores críticos para obter competitividade.

1. INTRODUÇÃO

A busca de vantagem competitiva pelas empresas através da valorização do ser humano e da adaptação de seus sistemas de informação para captação, tratamento, distribuição, disseminação e troca de informação no ambiente *internet/intranet/extranet*, vêm ocasionando o aparecimento de organizações baseadas na informação e no conhecimento. Tais organizações aproveitam de tecnologias para compartilhar o conhecimento entre todos os que participam do processo de dinamizar o negócio, ou seja, o capital humano (ou intelectual) da empresa.

Dentro desse contexto, os sistemas de informações gerenciais assumem um papel crítico no suporte à tomada de decisão, pela disponibilização de informação gerencial para o nível executivo, através de uma arquitetura de informação composta por ferramentas de análise e a apresentação da informação

(Sistemas de Informação Executivas, EIS) e de gerenciamento, recuperação e armazenamento da informação (*data marts, data warehouse*), sistemas transacionais, que utilizam tecnologias de processamento analítico, transacional e mineração dos dados (OLAP, OLTP e *data mining*, respectivamente), além das ferramentas de gestão integrada (ERP).

Porém, a postura dos usuários e a segurança das informações contidas nas bases de dados (*data warehouses*) ou nos sistemas de informações gerenciais passam a ser fatores críticos para se alcançar a efetividade gerencial e para manter a posse de seus maiores bens: a informação e o conhecimento.

O presente artigo pretende apresentar o novo modelo de arquitetura de informação, o novo cenário de distribuição e disseminação da informação, abordar questões relativas à necessidade de segurança e enfatizar a questão comportamental do usuário da informação.

2. NOVO MODELO DE ARQUITETURA DE INFORMAÇÃO

Nesse novo contexto, a informação é vista como estratégica. A tecnologia de informação é o ferramental necessário para usufruir e usar a informação para ser competitivo.

A evolução conceitual e tecnológica dos últimos tempos provocou uma evolução no conceito de arquitetura de informação, gerando uma nova abordagem no tratamento e infraestrutura tecnológica de suporte a gestão estratégica da informação nas organizações (Figura 1). Incluindo conceitos e tecnologias como OLTP, OLAP, *Data Mining*, EIS, ERP, *data warehouse*, a organização, sob a ótica da gestão da informação, pode ser dividida em dois níveis: (1) o operacional – responsável pela manutenção das atividades e o registro das transações diárias; e (2) o tático/estratégico – responsável pela visão e planejamento futuro das ações, que utiliza as informações já consolidadas e ferramentas de análise como suporte à tomada de decisão.

Nesse cenário, o *data warehouse* é, literalmente, um grande armazém organizado que fornece dados e informações aos sistemas gerenciais. Além disso, há um vislumbramento de democratização das informações gerenciais departamentais, e um achatamento dos níveis organizacionais (downsizing), além de uma tendência no mercado de sobreposição das características e funções segundo o apoio à

decisões, e sua relação com os níveis hierárquicos da organização (segundo Laudon & Laudon, 1996: ESS, MIS, DSS, KWS, OAS, e TPS).

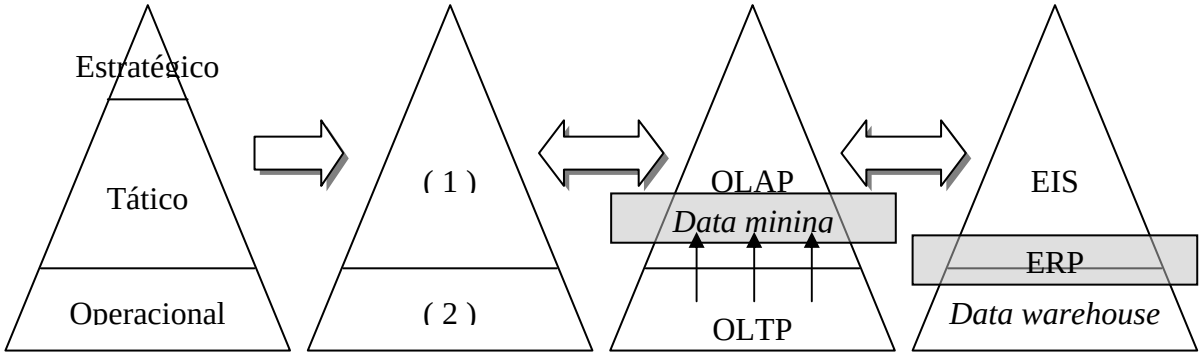

Figura 1: arquitetura da informação e as novas filosofias e tecnologias (Carvalho, 1999).

No nível gerencial e segundo a ótica da gestão da informação e o respectivo suporte da tecnologia houve, portanto, uma fusão das camadas tática e estratégica, formando assim uma só camada, possível a partir do suporte de ferramental específico, descrito a seguir.

2.1. DEFINIÇÕES BÁSICAS DE OLTP, OLAP E DATA MINING

O OLTP (*On-Line Transaction Processing*) e o OLAP (*On-Line Analytic Processing*) constituem-se em uma recente abordagem do que se pode fazer com relação aos sistemas de informação como suporte à tomada de decisão.

Segundo Brackett (1996), *On-Line Transaction Processing* é "o processamento que suporta as operações de negócio diariamente. Também é conhecido como processamento operacional e OLTP". Ainda segundo o mesmo autor, *On-Line Analytic Processing* é "o processamento que suporta a análise da tendência e projeções do negócio. Este último também é chamado de processamento de suporte a decisão e de OLAP".

Inmon (1997) aborda que a noção de tempo de resposta no acesso a informações no ambiente OLAP é bem diferente do OLTP. Ambos dão suporte aos níveis operacionais e gerenciais (tático + estratégico), mas o tempo de resposta para o OLTP geralmente é medido em segundos e minutos, sendo por isso

considerado um fator crítico nesse ambiente. Já no OLAP não ocorre um relacionamento tão direto, fazendo com que este fator deixe, dessa forma, de ser crítico, pois o tempo de resposta nesse ambiente pode ficar em torno de horas, e até em dias. As razões que explicam esta diferença de enfoque nos fatores críticos para desempenho dos bancos de dados são: demandas e necessidades diferentes em termos de suporte à decisão para os dois níveis organizacionais descritos (1) e (2).

O OLTP trabalha com dados que movimentam o negócio em tempo real e o OLAP trabalha com dados históricos para gerar informações para analisar o negócio. O OLTP, então, passa a ter a função de alimentar uma base de dados, a qual o OLAP a utilizará para a "transformação do conteúdo em uma forma útil de informações que possam ser entregues a um grande número de usuários. Os documentos OLAP – representação de dados em relatórios e gráficos – são criados 'dinamicamente' (o aspecto 'on-line' do OLAP) para atender às necessidades de informação do usuário" (Harrison, 1998).

O OLAP, em geral, executa cinco funções básicas, que são: de interface, de consulta, de processo, de formato e de exibição. Deve proporcionar capacidades analíticas nas áreas de consulta e relatório, análise multidimensional, análise estatística e *data mining*. (Harrison, 1998).

Na consulta e relatório, deve ser capaz, por exemplo, de fornecer relatório de status (quais foram as vendas do último mês?), contagens (quantos clientes pagaram em cheque?) e lista (que clientes tiveram cheques devolvidos?). Na análise multidimensional, deve proporcionar a flexibilidade analítica para responder a questões como: Como o marketing afetou as vendas?, Onde devem ser realizadas novas incursões?, Que produto deve ser mais valorizado? e Quais clientes são não confiáveis?. Na análise estatística, dentre outras coisas, procura-se respostas a perguntas do tipo "E se ... ?". Já No Data Mining são utilizadas técnicas mais específicas.

Enquanto se projetam armazéns de dados históricos (*data warehouse*) para fornecer a memória da empresa, o *data mining* (mineração de dados) explora e analisa essa memória para produzir o conhecimento, a inteligência, aproximando-se da necessidade empresarial. Isso é feito através de meios automáticos ou semi-automáticos. Emprega-se técnicas de estatística, da ciência da computação e de inteligência artificial para realizar tarefas como classificação, estimativas, previsões, agrupamento por afinidade, reunião e descrição.

Dentre alguns fatores para se implementar o *data mining*, destaca-se: 1. Os dados estão sendo produzidos; 2. Os dados estão sendo armazenados; 3. O poder da computação está disponível a preços acessíveis; 4. A pressão competitiva é forte e 5. Os *softwares* de *data mining* comerciais tornaram-se disponíveis. (Harrison, 1998).

Com relação às técnicas utilizadas, cita-se: 1. Análise de seleção estatística; 2. CBR (raciocínio baseado em caso); 3. Algoritmos genéticos; 4. Detecção de agrupamentos; 5. Análise de vínculos; 6. Árvores de decisão e indução de regras; 7. Redes neurais artificiais e 8. Visualização.

2.2. DEFINIÇÕES BÁSICAS DE DATA WAREHOUSE, ERP E EIS

Segundo Inmon (1997), "*data warehouse* é um conjunto de dados baseado em assuntos, integrado, não volátil, e variável em relação ao tempo, de apoio às decisões gerenciais".

O *data warehouse*, na grande maioria das vezes, utiliza as bases de dados do nível operacional para construir um sistema de dados históricos em forma bruta ou razoavelmente resumidos.

Essa nova filosofia de armazenamento de dados vem sendo proposta para substituir as diversas bases de dados não integradas existentes nas organizações que geram relatórios imprecisos, dados redundantes e desconexos, dentre outros, que proporcionam uma ineficiência global das ferramentas de suporte à tomada de decisão.

Os principais clientes de um *data warehouse* são aqueles que tomam ou que auxiliam na tomada de decisão. Dentre esses, pode-se citar: gerentes, de um modo geral, e analistas de SAD (Sistemas de Apoio à Decisão).

Um Sistema de Informações Executivas (EIS) pode ser definido como um sistema computadorizado que fornece ao executivo um fácil acesso a informações internas e externas que são relevantes para os fatores críticos de sucesso de seu trabalho. Os EIS's devem ser personalizados, desenvolvidos para usuários executivos individualmente. Eles devem extrair, filtrar, comprimir e localizar dados críticos, prover acesso a status em tempo real, análise de tendências, relatórios de exceção, acesso e integração a uma vasta amplitude de dados externos e internos. Eles também devem ser amigáveis ao usuário e

requererem um mínimo ou nenhum treinamento para utilização, devem ser usados diretamente por executivos sem intermediários e apresentar gráficos, tabulações e/ou informações textuais.

Enterprise Resource Planning – ERP, planejamento de recursos empresariais, constitui numa abordagem sistêmica de tratamento da informação. Dentro de um único sistema ficam armazenadas informações acerca de recursos humanos, finanças, manufatura, manutenção industrial, suprimentos e materiais, vendas e distribuição, por exemplo. Todas as informações integradas em uma única base de dados, de informação. (Haberkorn, 1999).

Atualmente sistemas como EIS (Sistemas de Informações Executivas) e ferramentas como ERP, OLAP (Processamento Analítico On-Line), além de *data marts* – que surgiram com o advento da filosofia de *data warehouse* –, estão buscando dados diretamente do ambiente operacional; gerando assim uma visão limitada à abrangência das bases nas quais se buscam os dados. Dessa forma, o *data warehouse* é proposto para proporcionar uma abrangência global e integrada para esses sistemas, ferramentas e bases específicas departamentais.

Assim, pode-se concluir que enquanto o OLTP se encaixa no contexto operacional, o OLAP fornece suporte ao nível estratégico e tático. Nesse contexto o ERP se encaixa entre os dois níveis, buscando o dado operacional e fornecendo a informação ao usuário. Já *data mining* constitui uma ferramenta fornecida pela tecnologia para recuperação das informações que podem fornecer ao executivo uma informação diferenciada, explorando melhor o potencial das bases de dados.

O ESS (Sistema de Suporte Executivo), uma derivação do EIS,2 possui um suporte para comunicações eletrônicas, uma capacidade de análise de dados e ferramentas organizadoras. Estas são ditas, "capabilidades" que não estão previstas para o EIS. Embora, na prática, a separação entre estes dois tipos de sistemas executivos está cada vez mais difícil de ser identificada, dado que as ferramentas vendidas no mercado são bastante complexas.

Segundo Watson *et al* (1991), as maiores pressões externas para a alta gerência decidir pelo desenvolvimento do EIS são, em ordem de importância para os executivos (segundo pesquisa): meio ambiente cada vez mais competitivo, meio ambiente externo mudando rapidamente, necessidade de ser mais ágil no procedimento de negócio com o meio externo, necessidade de acessar bancos de dados

externos e mudanças ocasionais nos regulamentos governamentais, dentre outras menos relevantes. Para as pressões internas, também em ordem de importância: necessidade de informações adequadas, necessidade de melhorar a comunicação, necessidade de acessar dados operacionais, necessidade de ajustar rapidamente o status nas diferentes unidades de negócio, necessidade de incrementar a eficácia, necessidade de poder identificar tendências históricas, necessidade de incrementar a eficiência, necessidade de acessar a base de dados da corporação e necessidade de informações mais acuradas.

O autor ainda comenta que os executivos podem ter acesso ao EIS, de casa, em viagens, em qualquer local que ele esteja, porém, deve haver uma preocupação com segurança, suporte e uma comunicação especial. E que, em média, são necessárias cerca de 04 pessoas para fazer parte da manutenção do EIS.

Observa-se que os itens relativos à eficácia e eficiência representam preocupações menores para os executivos pesquisados. Contudo, se no desenvolvimento/manutenção de um EIS não forem focadas a eficiência e a eficácia gerenciais, não se atingirá aqueles fatores considerados prioritários pelos executivos: meio ambiente cada vez mais competitivo e a necessidade de informações adequadas.

3. NOVO CENÁRIO DE DISTRIBUIÇÃO E DISSEMINAÇÃO DA INFORMAÇÃO

Paralelo ao surgimento desses sistemas de armazenamento e tratamento de informações, o meio de disseminação e distribuição dessas informações que vem se destacando é baseado em redes de computadores utilizando protocolo TCP/IP – definição de *internet*, *intranet* (quando se refere ao meio interno de uma organização), e *extranet* (quando se conecta redes distintas em longa distância).

A crescente utilização dessa tecnologia (*internet/intranet/extranet*) para disseminar e distribuir informações fez ampliar a preocupação com a segurança e a confiabilidade das informações vitais para a empresa. Antes do surgimento dessa tecnologia, as preocupações com segurança se limitavam a espionagem industrial, a fraudes, a erros e acidentes, entre outros. Atualmente há a preocupação com *hackers*, invasões, vírus, “cavalos de tróia”, espionagem eletrônica (*sniffers*), falsificação de identidade (*spoofing*), etc.

Em uma pesquisa realizada em 206 empresas de grande porte pela Módulo (Bastos, 1998), constatou-se que o uso da *internet* passou de 29% em 1996 para 63% em 1997, e o uso da *intranet* passou de 3% para 49% nesse mesmo período. Entretanto, os investimentos em proteção e controle não acompanharam esse crescimento: 82% não possuem política de uso da *internet*, 12% sofreram algum tipo de ataque, e 45% não sabem dizer se sofreram invasão.

Segundo outra pesquisa, feita pela CSI (*Computer Security Institute*) (Grego, 1998): 75% das empresas (equivalente a 249 empresas) tiveram perdas por falhas de segurança que juntas somaram 100 milhões de dólares em 1997.

Assim, a segurança deveria ser preocupação desde a etapa de planejamento dos sistemas de informação que utilizam a *intranet* como meio. Isso porque, com o avanço da tecnologia de banco de dados em geral, ao invés de se ter acesso apenas a leitura, passou-se a poder realizar inserções e atualizações com maior facilidade. Além disso, ferramentas de acesso privilegiado como o OLAP (que permitem acesso a todos os níveis do *data warehouse* ou sistema de informação equivalente) podem proporcionar a busca de informações não autorizadas.

A segurança do banco de dados está voltada, basicamente, para a proteção da integridade dos dados do *data warehouse*. Uma estratégia para melhorar o nível de segurança dos dados confidenciais, ou não, seria separar os sistemas operacionais (OLTP) do *data warehouse*. Assim, mesmo que se acesse/viole o *data warehouse*, os dados operacionais, que são os críticos já que suportam as operações diárias das organizações, estarão protegidos e inacessíveis.

Outra estratégia de limitar o acesso não autorizado e a violação de informações seria fazer *data marts* (bases departamentais) com informações resumidas para evitar expor o *data warehouse* na *intranet*, ou seja, expor os *data marts* e “esconder” o *data warehouse* da rede interna e externa.

Entretanto, independente da estratégia adotada, por medida de segurança o administrador da rede deve conferir aos usuários permissões e restrições para executar os comandos de acesso padrão a banco de dados – SQL (*select, insert, update, delete,* e *reference*) –. Além disso, deve-se criar também níveis de acesso para ferramentas como o OLAP. Deve-se ainda diferenciar senha de acesso à rede de senha de acesso aos sistemas de informações, ao *data warehouse*, e à ferramentas como o OLAP.

Comparando com uma corrente, a questão da segurança das bases de dados e dos sistemas de informações como um todo não representam o elo mais fraco. Este elo é a segurança nos servidores *intranet* e *internet*, nas estações clientes, no meio de transporte, e na rede interna como um todo. Estes são os pontos mais críticos que podem ocasionar em perda e roubo de informações. (Bastos, 1998)

A segurança das informações nas empresas devem receber, portanto, tratamento comparável ao que a segurança do patrimônio físico recebeu nas últimas décadas. Esse tratamento deve ser ainda maior quando se tem que a informação é, juntamente com as pessoas (capital humano), o maior patrimônio da empresa. Por isso, o setor de informática da empresa, que controla os meios de armazenamento e distribuição das informações, deve atuar também como um setor de "vigilância". Proteger a informação das empresas é condição vital para a existência das mesmas.

As pessoas que ocupam o setor de informática de uma empresa ou a equipe que gerencia os sistemas de informação não precisam ter conhecimentos específicos desse novo cenário. Mas deve ser preocupação da alta gerência que os profissionais que gerenciam o controle e a distribuição das informações tenham uma visão global do valor que cada tipo de informação agrega ao capital da empresa, e atuar como gerentes supervisores das empresas terceirizadas, que por ventura existirem, que estiverem implementando a segurança e os sistemas de informações na empresa.

4. NECESSIDADES DE SEGURANÇA

As necessidades básicas de segurança da rede são: (Bernstein *et al*, 1996)

1. Confidenciabilidade – assegurar que as trocas de informações sejam privadas;
2. Integridade – garantir que a mensagem em trânsito permaneça inalterada; e
3. Autenticação – verificar a veracidade daqueles que desejam realizar transações.

Dentre os tipos de ameaças e ataques freqüentes, destaca-se: (Bernstein *et al*, 1996)

1. A espionagem (*sniffers*) pela captação de todo o tráfego de informações que passa pela rede;
2. O disfarce (*spoofing* de IP) através de exploração de falhas no protocolo de rede IP (*Internet Protocol*);

3. Execução de aplicações não autorizadas (“cavalos de tróia”) que pode produzir resultados indesejáveis como perda ou repasse de informações;
4. Repúdio ou negação de participação em transações;
5. Negação de serviço, como tirar um servidor do ar, por exemplo;
6. Exploração de senhas, através de tentativas de acesso ou exploração do arquivo de senhas; e
7. Engenharia social, técnica que utiliza a psicologia para obter informações dos próprios funcionários da empresa vítima utilizando da confiança adquirida com os mesmos.

4.1. SEGURANÇA NO MEIO DE TRANSPORTE

Para promover a segurança no meio de transporte dos dados, pode-se utilizar a criptografia para garantir a privacidade, a integridade, e o não repúdio.

A criptografia utiliza algoritmos matemáticos para codificar uma mensagem. Para decodificar uma mensagem de forma não autorizada é necessário uma determinada capacidade computacional. O governo americano limitou o grau de criptografia dos *softwares* produzidos e exportados dos EUA. Com isso, associado ao evento da capacidade computacional disponível a um número cada vez crescente de pessoas, fica fácil decodificar mensagens normais trocadas pelos navegadores (*browsers*) utilizados na *internet/intranet/extranet*.

Para assegurar a transação confiável, são utilizadas técnicas que fazem com que a forma de codificação mude antes que se consiga decodificar a mensagem.

Uma solução, de baixo custo, para pequenas, médias e grandes empresas que queiram utilizar do meio inseguro da *internet* para interligar escritórios, filiais, fornecedores, clientes, e/ou funcionários de forma segura, é a utilização da chamada VPN (Rede Virtual Privada). A VPN cria “túneis” de criptografia de alto grau de codificação, fazendo com que as transações sejam confiáveis e o acesso às bases de dados sejam seguros.

A autenticação, aliada à criptografia, deve prover a identificação correta de quem está acessando o sistema. Para isso são utilizados mecanismos como: (Bernstein *et al*, 1996)

1. Identificação Biométrica – que utiliza as formas do corpo humano, como a íris do olho ou a impressão digital como identificação;
2. *Callback* – quando se conecta ao servidor, há uma desconexão e a ligação é retornada pelo mesmo;
3. Identificação de Chamada – do número telefônico, por exemplo;
4. Identificação do nó de rede, a qual se está conectado;
5. *PC Cards* – que se encaixa no computador. Autenticação via *hardware*;
6. *Smart Cards* – usa cartão magnético, ou códigos de barra com identificação pré-definida;
7. Dispositivos de *Token* – funciona parecido com *smart cards*, com a diferença de não estar ligado fisicamente e necessitar do usuário para autenticar;
8. Senha Ocasional – é fornecida uma senha momentânea cada vez que o usuário tenta se autenticar com a senha tradicional;
9. Senha Tradicional – forma mais comum de autenticação. É fornecida ou definida pelo usuário para utilizar o sistema.

4.2. SEGURANÇA NO SERVIDOR

A problemática da segurança no servidor é a possibilidade de roubo de informações e o risco do uso e do acesso indevido das mesmas.

Os *firewalls* são as soluções utilizadas para controlar os servidores e os acessos permitidos, monitorar o uso e as tentativas de violações, proteger os servidores contra invasões externas, e possibilitar a realização de auditorias.

Deve haver uma preocupação com relação à detecção de incidentes e a contratação de pessoas externas, com supervisão da empresa contratante, para tentar descobrir falhas de segurança.

4.3. SEGURANÇA NA ESTAÇÃO CLIENTE

É considerado um dos pontos mais vulneráveis da rede, onde o usuário, através de uma aplicação dedicada ou um *browser*, tem acesso aos recursos e aos serviços da rede. As estações podem armazenar informações pessoais sem proteção ou controle de acesso.

Os *browsers* podem permitir, por exemplo, a execução de programas desconhecidos que podem atuar como “cavalos de tróia”, a possibilidade de fazerem grampos de teclado, ou outras armadilhas de acesso.

As pessoas que gerenciam as informações devem ter consciência de que quanto maior a necessidade por segurança, maior a complexidade para autenticação do usuário no sistema, dificultando a usabilidade do referido sistema. No entanto, o custo e a usabilidade do sistema pelo usuário devem ser considerados de grande importância no planejamento da segurança da informação, dado que o custo da perda ou do vazamento dessa informação pode atingir cifras incalculáveis.

4.4. SEGURANÇA NA REDE INTERNA

Segundo uma pesquisa recente da *WarRoom Survey* (Bastos, 1998) sobre a natureza dos ataques, constatou-se que 61% das organizações sofreram ataques *internos* em 12 meses, sendo que em 45% dos casos foram registrados perdas de até US$ 200.000,00 e em 15% perdas de até US$ 1.000.000,00.

O intruso pode almejar ganhos financeiros, vingança, necessidade de aceitação ou respeito, curiosidade ou busca de emoção, anarquia, aprendizado, espionagem industrial, espionagem nacional entre outros.

Percebe-se, portanto, que o “inimigo” geralmente está mais dentro do que fora da empresa. Assim, deve haver estratégias para controlar o uso e os acessos internos.

Nesse contexto deve ser definido uma política interna que defina o grau de sigilo de cada informação, quais dados serão disponíveis, quem da empresa pode ter acesso aos dados, e como será feito esse acesso nos diferentes níveis hierárquicos e departamentais sem comprometer a socialização, o compartilhamento e a distribuição das informações.

5. MUDANÇA DE COMPORTAMENTO

Não é tarefa fácil para a equipe de informática e/ou a equipe que gerencia os sistemas de informações associar tudo que deve ser feito de modo transparente ao usuário final. Para isso é importante uma política de conscientização para o uso adequado, racional e responsável dos sistemas da empresa. Os recursos de acesso às informações devem ser valorizados pelas pessoas da mesma forma que elas tratam suas contas bancárias, por exemplo. Afinal, é na informação que, cada vez mais, está sendo concentrado o capital da empresa; e a segurança desse capital é uma questão de sobrevivência no atual cenário competitivo.

As *extranets/intranets/internet* estão atraindo cada vez mais novos negócios e mercados. A existência de riscos e vulnerabilidades a que se está exposto deve ser do conhecimento de todos que lidam com o meio, e devem ser definidos mecanismos adequados para a segurança.

É necessário uma mudança radical no comportamento das pessoas quando do uso dos sistemas. Um bom começo é ter consciência sobre a responsabilidade da senha individual de acesso aos mesmos. Deve haver um mínimo de colaboração de todos.

Não basta seguir as tendências de mercado deixando-se levar pelas enormes vantagens de se disponibilizar sistemas de informações, *data warehouse*, ou *data marts* na *intranet/internet/extranet*, sem se preocupar com a segurança do dado/informação.

Sem uma boa política de segurança e uma identificação de riscos, não vale a pena se aventurar nesse ambiente, podendo perder, irresponsavelmente e/ou negligentemente, informações secretas e/ou valiosas para os concorrentes.

Os prejuízos decorrentes do vazamento de informações podem pôr em jogo o negócio da organização. Porém a não incursão nesse novo contexto pode significar a incapacidade de continuar no mercado.

Portanto, torna-se imperativo uma mudança de postura e de comportamento de todos: daqueles que projetam, daqueles que usam e, principalmente, daqueles que gerenciam os sistemas; pois são desses últimos que deve vir o exemplo e a conscientização iniciais.

Mudanças de comportamento como um fenômeno organizacional tomam tempo e não são espontâneas. Requerem a definição de uma estratégia clara, que leve em consideração vários fatores, além de conscientização do usuário para a necessidade por segurança e a importância da informação para a sobrevivência do negócio da empresa.

Uma organização para atingir seu objetivo deve dar "sinais" claros da importância do "capital humano" que ela detém; deve buscar a satisfação dos seus colaboradores com o ambiente no qual trabalham.

Para lidar com o fator tempo (mudanças de comportamento levam tempo para se efetivarem como um fenômeno organizacional homogêneo), é necessário que a organização estabeleça metas parciais no desenvolvimento da própria infraestrutura de informática de suporte aos negócios (*data marts*, *data warehouse*, EIS, *intranet*, etc...). Metas parciais indicam progresso, mostram resultados concretos e estabelecem uma relação de custo/benefício positiva, conquistam o usuário e o suporte da alta gerência, disseminando uma cultura voltada para a integração e padronização de dados e para a segurança.

6. BIBLIOGRAFIA

BASTOS, Alberto. Informação Segura na Internet e Intranet: Oportunidade x Risco. IN: Revista Developers Maganize, Rio de Janeiro: Editora Axcel. Ed. fevereiro. pp. 44-45, 1998.

BERNSTEIN, Terry, BHIMANI, Anish B., SCHULTZ, Eugene, SIEGEL, Carol A. Segurança na Internet. Rio de Janeiro: Campus, 1997. (ISBN 85-352-0140-8).

BRACKETT, Michael H. The Data Warehouse Challenge: Taming Data Chaos. USA: Wiley, 1996. (ISBN 0-471-12744-2).

GREGO, Maurício. A Insegurança Bate à Porta. IN: Revista Info Exame, São Paulo: Editora Abril. Ed. março, pp.98, 1998.

HABERKORN, Ernesto M. Teoria do ERP – enterprise resource planning. São Paulo: Makron Books, 1999.

HARRISON, Thomas H. Intranet Data Warehouse. São Paulo: Berkeley, 1998. (ISBN 85-7251-460-0).

INMON, W. H. Como Construir o Data Warehouse. Rio de Janeiro: Campus, 1997. (ISBN 0471-14161-5).

LAUDON, K. C., LAUDON, J. P. Management Information Systems: Organization and Technology. New Jersey: Prentice Hall, 1996, 4ª edição. (ISBN 0-13-213778-X)