33 – Junho de 2001

Segurança da Informação: lendas e verdades

Considerando que os aspectos relacionados a Segurança da Informação transcendem a esfera tecnológica, atribuindo igual relevância aos aspectos físicos e humanos; considerando que há muito venho escrevendo sobre gestão corporativa e os momentos vividos pela informação em seu ciclo de vida: manuseio, armazenamento, transporte e descarte; considerando que a invasão ocorre onde o controle falha, e ainda que pequenos descuidos podem comprometer todo o trabalho e investimento realizado em busca da redução dos riscos, resolvi quebrar a rotina da coluna e escrever algo ainda mais didático e prático visando eliminar dúvidas, ratificar verdades e derrubar lendas associadas ao assunto.

O Firewall tem papel importante na proteção da rede.

O firewall é um importante elemento no esquema de proteção da rede de computador, mas deve estar adequadamente configurado a fim de bloquear eficientemente as informações que entram e saem da rede, sem que isso represente transtornos de queda de performance e redução de flexibilidade que acarretem na inoperância ou indisponibilidade de informações.

Basta ter um Firewall para estar protegido.

O firewall não pode ser encarado como "o salvador da pátria", pois cumpre – se bem configurado - apenas um papel pontual de bloqueio de acessos lógicos seguindo regras de filtragem previamente determinadas. Deve ser constantemente auditado e monitorado servindo de sinalizador de novas situações de risco e novas necessidades de configuração e bloqueio. DICA: Firewall Products Search Center - http://www.spirit.com/cgi-bin/report.pl

O Personal Firewall complementa os demais mecanismos de segurança de rede.

Mesmo contando com outros dispositivos de segurança de rede como: roteador com filtro, *Intrusion Detection System* etc, é cada vez mais comum e conveniente se proteger com a instalação de programas chamados Firewall Pessoal. Eles oferecem mais uma camada de filtro à estação, permitindo personalização e controle sobre o compartilhamento de arquivos e serviços. Não se trata de um mecanismo infalível, e sim mais um dispositivo que corrobora com o desafio de redução dos riscos.

O Personal Firewall atrapalha o uso do computador.

Assim como no Firewall de Rede, precisa de uma configuração contextualizada de acordo com as necessidades de acesso do usuário, evitando bloqueios indesejados e a indisponibilidade de informações e acessos. DICA: existem programas bons e gratuitos que podem ser encontrados em www.zonealarm.com e www.blackice.com

Vírus não contaminam apenas tradicionais arquivos auto-executáveis.

Vírus são também transmitidos por arquivos que contenham texto, como os em formato Word. Isso por que o Word dispõe de uma linguagem de programação chamada de MACRO que pode ser usada para se desenvolver e escrever um vírus de computador. Além disso, arquivos que contenham texto que representem comandos HTML anexados ao e-mail, usados na Internet, podem conter pequenos programas em linguagem Java Script com intenções maléficas que acabam automaticamente executados pelos principais programa de e-mail do mercado. DICA: Symantec Antivirus Research Center - http://www.symantec.com/avcenter/

Trojan Horse são vírus modernos.

Trojan Horse não são vírus, apesar de serem rastreados e eliminados pelos principais programas antivírus do mercado. Uma parte do programa (server) se instala na máquina da vítima depois que a mesma executa algum programa "contaminado". Este processo ocorre sem que o usuário perceba e, depois de concluído, dá controle total do computador ao invasor que dispõe de outra parte do Trojan Horse (client).

Certificados Digitais são uma tendência global para autenticação.

Os Certificados Digitais construídos por um par de chaves pública e privada, possibilitam a autenticação de informações, acessos e serviços a partir de uma assinatura digital resultante de seu uso. Aplicáveis nas mais diversas iniciativas como: B2B, B2C, Sistemas ERP, e-commerce, e-publishing, Desktop Protect, Intranet, Extranet, e-mail etc, viabilizará a identificação das partes e ainda servirá de mecanismo de responsabilização civil – havendo respaldo legal – para que tenhamos os relacionamentos eletrônicos máquina-homem, máquina-máquina e homem-homem autenticados e possivelmente reconhecidos globalmente. PKI ou Public Key Infrastruture é a tecnologia promissora que representa a luz no fim do túnel para viabilizar a administração da enxurrada de certificados que estarão sendo usados em toda e qualquer troca eletrônica de informações nos próximos anos no mundo. DICA: conheça mais sobre a tecnologia e sua aplicabilidade visitando www.modulo.com.br e www.entrust.com

Acessar um site com certificado digital é sinal de proteção.

O uso de certificado digital por si só, não garante a proteção do usuário, pois é preciso ainda verificar a validade do certificado do site, a credibilidade da empresa que o emitiu e ainda se foi emitido para o site verdadeiro. Nada impede que um site falso, que se faça passar por um loja eletrônica, por exemplo, tenha um certificado digital usado para autenticá-lo e ainda para criptografar as informações que trafeguem entre o usuário e o site. Além disso, mesmo depois de verificada a veracidade do site, do certificado e da autoridade certificadora, e a garantia de confidencialidade das informações trocadas com o uso da criptografia, não podemos esquecer que as mesmas ainda serão armazenadas eletronicamente em um banco de dados ou ainda fisicamente, depois de impresso, em alguma pasta arquivo. Portanto, procure conhecer melhor os mecanismos adotados pelo site e seu comportamento quanto ao processo de gestão das informações em todo seu ciclo de vida. DICA: se estiver usando o browser Internet Explorer, dê um clique duplo na imagem do cadeado que se fecha no pé da página quanto o site possui e usufrui de um certificado digital. Assim, saberá as informações relacionadas.

 **Pode ser seguro usar o Correio Eletrônico.**

A criptografia é um dos elementos que viabilizam o uso do correio eletrônico com altos índices de confidencialidade e segurança. Esta pode ser facilmente usada a partir da adoção do certificado digital que depois de instalado em seu computador – seguindo alguns poucos passos indicados pela autoridade certificadora que o emitiu – é explorado pelos principais programas de e-mail disponibilizando dois botões: um para assinar digitalmente o e-mail e outro para criptografá-lo. Este último necessita da chave pública do destinatário para ocorrer, portanto, tanto destinatário quanto remetente terão de possuir um certificado digital. DICA: Adquira um certificado digital para e-mail (classe 1) por uma anuidade acessível em sites especializados.

 **O e-mail corporativo não oferece riscos as informações veiculadas.**

Perigoso engano. Apesar de aparentemente mais seguro por estar em ambiente controlado e privado, um e-mail sem criptografia é tão "seguro" quanto um cartão postal escrito a lápis encaminhado pelo correio tradicional, ou seja, não há garantia de confidencialidade de seu conteúdo, bem como de sua integridade. Além disso, um ponto comumente esquecido, muito comum e altamente perigoso é a forma com que os programas de e-mail estão configurados para checar a caixa postal. Este processo costumeiramente ocorre através do protocolo POP – Post Office Protocol que, usado toda vez que a checagem é acionada, encaminha um pacote de dados com sua senha da caixa postal em claro, ou seja, sem criptografia. DICA: o problema pode ser sanado configurando e habilitando o serviço padrão SSL – Security Socket Layer, tanto no server quanto no client, que irá proteger com criptografia sua senha sempre que a mesma estiver trafegando na rede em função de mais uma das centenas de checagens que fazemos diariamente.

 **Senhas precisam ser definidas com base no contexto.**

As senhas devem ser construídas considerando o valor da informação e ativo protegidos, o tempo em que a mesma estará cumprindo esta tarefa, e o interesse e poderio dos interessados em burlá-la. É conveniente misturar letras em maiúsculo, minúsculo, números e caracteres especiais para se obter uma senha complexa mais forte. DICA: Construa uma frase como: "Minhas férias de 98, inverno, foram na Itália." e construa a senha a partir dela: Mfd9,i,fnI. Procure memorizar...ao menos a frase. ☺

 **É mais prático é seguro possuir uma única senha forte.**

Este comportamento, apesar de comum, é estritamente condenável. Funciona como se contássemos um segredo para dezenas de pessoas, tendo de contar com a confiança de todas elas para que o segredo não vaze. É conveniente construir senhas com grau de complexidade (tamanho e formação) em função do que está sendo protegido, e ao menos (se não quiser adotar uma senha para cada tipo de acesso) segmentar os tipos de acesso de acordo com sua importância. Por exemplo: uma senha para o banco A, outra para o banco B, uma para o correio eletrônico, uma outra só para sites que não armazenem informações pessoais valiosas etc. DICA: utilize a dica anterior para criar uma senha Mestre que será usada por você para criptografar um arquivo eletrônico contendo todas as demais senhas que possui. Apenas memorize-a.

 **Antivírus automatizado agrega mais segurança.**

Em virtude da velocidade impressa pela Internet e consequentemente da evolução dos vírus de computador, torna-se coerente adotar programas antivírus que se atualizem automaticamente e ainda façam o rastreamento automático de arquivos quando estes foram manipulados e até mesmo quando chegarem anexados ao correio eletrônico.

Atualizando meu antivírus todo mês estou seguro.

Existem aproximadamente 51 mil vírus de computador diferentes - conforme pesquisa norte-americana feita no ano 2000 - espalhados pela grande rede Internet. Assim, atualizar o antivírus numa periodicidade mensal já não é suficiente para protegê-lo das versões mais novas e potencialmente cada vez mais perigosas.

Um projeto Análise de Segurança deve ir muito além da análise tecnológica.

Outrora o mesmo era visto apenas por uma análise superficial – muitas vezes realizada por *software scanner* - dos ativos tecnológicos como servidores, sistemas operacionais, roteadores e links. Felizmente, agora a percepção mais ampla e completa está virando *comodities*, onde se realiza uma análise muito mais profunda também dos aspectos físicos como: infra-estrutura predial, cabeamento estruturado, combate a incêndio etc, e dos aspectos humanos que através de entrevistas e análises de documentos, consideram a cultura dos funcionários a fim de auxiliar a identificação das vulnerabilidades, ameaças, riscos e impactos.

Política de Segurança é tudo igual e pode ser copiada de empresa bem sucedida.

Se considerarmos verdadeira a premissa de que cada empresa tem particularidades relacionadas a ameaças, riscos, impactos, recursos tecnológicos, físicos e até mesmo características culturais, concluímos que a solução corporativa de segurança deve ser igualmente personalizada. Com a Política de Segurança, um dos importantes componentes da solução, não poderia ser diferente. Este deve refletir critérios contextualizados alinhados com os desafios e as estratégias de empresa. Para tal, deve-se escrever diretrizes, normas, procedimentos e instruções próprias, de forma a adequar as necessidades específicas da empresa aos desafios de segurança da informação. DICA: por se tratar de um documento extenso e complexo, inicie os trabalhos especificando as diretrizes básicas de segurança que irão nortear posteriormente as normas, procedimentos e instruções.

Testes de Invasão amadores podem pôr em risco sua empresa.

Infelizmente não é esta a visão de todos. Um Teste de Invasão deve ser tratado com a seriedade de um projeto, onde serão especificados os alvos, objetivos, prazos, técnicas e ferramentas, acompanhado de uma autorização e o possível acompanhamento dos funcionários da empresa. Apesar de comumente demandar pouco tempo para sua realização, o mesmo deve ser executado por profissionais qualificados a fim de dar veracidade adequada ao teste, e sem expor as informações da empresa em virtude de falhas humanas e perda de controle que normalmente ocorrem com ações amadoras.

Seguir uma Norma de Segurança é garantia de sucesso em projetos de segurança.

As Normas de Segurança, especificamente a BS7799 e a sua versão internacional ISO 17799-1, têm papel importante nas ações corporativas de segurança em busca de conformidade, mas não podem ser encaradas como “a fórmula” de sucesso, pois além de superficiais, se limitam a apontar O QUE fazer e não COMO fazer. Deve haver sempre

uma metodologia *compliant* capaz de materializar as ações garantindo o sucesso de cada projeto e atividade da Solução Corporativa de Segurança da Informação. DICA: leiam as normas mencionadas acima e busquem uma metodologia de execução que esteja em conformidade.

 **Engenharia Social é tão perigosa quanto uma invasão via Internet por um hacker.**

Muitas são as técnicas e ferramentas para se obter acesso indevido à informação, esteja ela em formato eletrônico, em papel etc. A técnica da engenharia social é muito utilizada para o levantamento de informações preliminares que possam tornar a tentativa de invasão mais eficiente. É preciso saber que de nada adiantará um alto nível de segurança no correio eletrônico, por exemplo, se o mesmo for posteriormente impresso, transportado, armazenado e até mesmo descartado sem o mesmo nível de segurança. DICA: treinamento maciço acompanhado da divulgação adequada da política de segurança da empresa, contribuem em muito para a repressão das tentativas de Engenharia Social.

 **IDC – Internet Data Center consideram todos os aspectos da Segurança da Informação.**

Acrônimo da moda, os IDCs estão tomando conta do mercado, permitindo que as empresas se dediquem exclusivamente ao seu *core business* sem se preocupar com as atividades meio, pois oferecem serviços de hospedagem, alta conectividade e contingência. Mas nem todos consideram completamente os aspectos de segurança visando garantir os índices de confidencialidade, integridade e disponibilidade. Têm de oferecer mais do que redundância de equipamento e infra-estrutura. Precisam complementar os tradicionais serviços com uma equipe especializada em segurança, que de forma presencial ou remota, mantenha continuamente um processo de gestão e monitoramento dos ativos, transformando o IDS em SIDC – Secure Internet Data Center. DICA: ao contratar os serviços de um IDC, procure identificar a existência de uma parceria com empresa especializada em segurança da informação, ou a formação de uma equipe própria de monitoramento 24 horas por dia, 7 dias por semana que garanta o "S" do IDC.

 **Segurança da Informação é controle.**

Se pudéssemos eleger uma palavra para resumir a amplitude do desafio associado à Segurança da Informação, esta seria: CONTROLE. A partir da especificação, configuração e implantação de controles físicos, tecnológicos e humanos preocupados com o manuseio, armazenamento, transporte e descarte das informações, consegue-se reduzir e administrar os riscos. DICA: segurança é adotar controles que visem administrar os riscos, fazendo-os tender a zero.

 **Minha empresa está segura.**

Por mais que tenha especificado os melhores controles para reduzir e administrar os riscos de quebra da confidencialidade, integridade e disponibilidade das informações, nunca estará totalmente seguro. À propósito, nem sempre todos precisam do mesmo nível de segurança, haja visto que as empresas – por mais parecidas, física, humana e tecnicamente – sempre possuem particularidades associadas aos riscos e impactos que são determinantes no momento de se especificar a melhor solução de segurança. Lembre-se: uma dose inadequada de segurança, seja alta demais ou baixa demais, poderá acarretar no primeiro

caso: em baixo retorno sobre o investimento, burocratização dos processos, perda do time to marketing, indisponibilidade, e no segundo caso: em ineficácia tática-operacional.

 **Segurança da Informação precisa ser tratada corporativamente.**

É fator crítico de sucesso tratar os problemas de segurança de forma ampla e completa, pois diferente disso, as empresas terão apenas soluções isoladas e pontuais que pouco contribuirão para elevar o nível de controle e segurança das informações da empresa. A coordenação corporativa e a sinergia entre as ações de diversas áreas garantirá maior retorno sobre o investimento e a manutenção do nível de segurança atingido.

 **PDI – Plano Diretor de Informática deve tratar da Segurança da Informação.**

Erro comum e persistente julgar atributo da área de TI o tratamento da segurança da informação. Como vimos, os problemas transcendem os aspectos tecnológicos e precisam de uma nova estrutura orçamentária e de gestão. Contar com um Comitê Corporativo Multidisciplinar de Segurança da Informação, a figura do Security Officer e um PDS – Plano Diretor de Segurança, torna-se primordial para que a empresa construa um verdadeiro processo de gestão de riscos.

 **O Security Officer é peça chave na coordenação de ações corporativas de segurança.**

O desafio de reduzir os riscos, elevar e dar manutenção no nível corporativo de segurança da informação não é responsabilidade de uma só pessoa, e sim de todos os funcionários. Contudo, o Security Officer tem o importante papel de priorizar e planejar atividades, e coordenar as ações de segurança que outrora ocorriam de forma isolada e sem sintonia, alinhando-as definitivamente com as estratégias de negócio da empresa. Comumente contando com o apoio de consultoria externa especializada, o Security Officer passa a ser o elo de ligação, absorção e disseminação da cultura de segurança de forma organizada e coerente com o PDS – Plano Diretor de Segurança.

 **Se me sinto seguro, estou seguro.**

Errado. A sensação de segurança é comumente causada pela falta de controle que lhe permita conhecer as vulnerabilidades, os pontos de perda e invasão. Esta situação acaba consolidada por soluções pontuais, isoladas e comumente de caráter técnico, que traz conforto momentâneo e a falsa sensação de segurança. Os números da última pesquisa de segurança da Módulo Security Solutions revelam um alto índice de desconhecimento e grande despreparo das empresas diante do vertical crescimento da informatização, digitalização, conectividade e compartilhamento. Muitos estão sentados em um barril de pólvora e nem ao menos sabem disso!

 **É coerente destinar um percentual do investimento em TI para segurança**.

Esta tem sido uma das formas mais indicadas para dimensionar o orçamento destinado aos investimentos em Segurança da Informação, pois há um crescimento vertiginoso do índice de informatização e principalmente conectividade das empresas, e esta evolução acaba diretamente relacionada ao aumento do grau de exposição e risco. DICA: o percentual tende a variar de acordo com o perfil do negócio, mas invariavelmente fica na faixa entre 5% e 25%, podendo ainda quebrar esta barreira em negócios críticos exclusivamente eletrônicos, e atingir o volumoso montante de 50%.

Todas as empresas que oferecem produtos e serviços de segurança são iguais.

Conclusão equivocada, mas que ainda persiste na cúpula de muitas empresas. Para eliminá-la de vez, precisamos entender que o mercado de segurança e os desafios atrelados a ele são extensos. Por isso, surgem diversas empresas que participam com a oferta de ferramentas e produtos específicos. São eficientíssimas substituiria por: no tratamento de situações pontuais e específicas, mas são deficientes quando pensamos no problema como um todo. Juntamente com estas, surgem as integradoras. Empresas que reúnem algumas peças fornecidas pelas primeiras, agregando serviços para formar produtos mais amplos, mas que continuam em uma esfera menor preocupadas com ambientes e processos específicos. Diferente de todas as demais, nascem empresas híbridas (consultora, integradora e desenvolvedora de software) preocupadas com a raiz da expressão "Segurança da Informação", ou seja, preocupada em especificar uma solução corporativa de segurança que viabilize a formação de um processo de gestão capaz de reduzir os riscos físicos, tecnológicos e humanos atrelados aos momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte. Possuem alta especialização técnica verticalizada em segurança da informação (pois este é seu *core business*) e, além de oferecer diversos componentes com atividades técnicas, estão intimamente interessados, ligados e preocupados com a sinergia destas com os desafios de negócio de seus clientes. Preocupadas em agregar valor à empresa e principalmente em viabilizar o maior retorno sobre os investimentos, fornecem a estrutura necessária para que possam tratar a segurança da informação corporativa de forma integrada como um processo e não simplesmente como um projeto. DICA: só depois de traçar seu cenário atual e o cenário desejado, inicie a avaliação das opções de parceria no mercado para que não se iludir com a sensação de segurança proporcionada por soluções estritamente pontuais e isoladas.

Plano Diretor de Segurança é um investimento de alvo valor agregado.

Em virtude da complexidade das empresas, heterogeneidade de tecnologias, desafios mercadológico-comerciais, e ainda pelo veloz crescimento da dependência da informação para gestão do negócio, torna-se fundamental planejar as ações de segurança e diagnosticar de forma corporativa as vulnerabilidades físicas, tecnológicas e humanas, sem desconsiderar a relevância e a sensibilidade de cada processo de negócio diante de uma possível quebra de segurança. Só através de um PDS – Plano Diretor de Segurança pode-se traçar uma estratégia coerente e alinhada com os interesses da empresa de forma a viabilizar a construção de um Modelo de Gestão Corporativa de Segurança da Informação. DICA: possuir um PDS é ter uma bússola que auxiliará o Security Officer e o Comitê Corporativo de Segurança da Informação a encontrar o caminho, apontando as prioridades e atividades mais pertinentes à empresa que busca seu nível de segurança adequado.

Verdades

Lendas

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente de Produto e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br