Segurança da informação nas pequenas empresas

Information security in small business

Paulo Leandro de Oliveira
pauloleandro23@gmail.com

Resumo

A segurança da informação é cada vez mais necessária nas organizações e exige sempre inovações e um acompanhamento dos gestores de TI, mostrando a importância que a informação traz ao negócio. Possibilita, ainda, estar sempre um passo à frente das ameaças e vulnerabilidades que possam comprometer o caminho dos gestores, os quais passam a ter em mãos uma política de segurança bem elaborada, firmando o compromisso com a confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

Palavras-chave: Segurança. Informação. Gestores. TI. Vulnerabilidades.

Abstract

Information security becomes increasingly necessary in organizations and always requires a follow-up of innovations and IT managers, always showing the importance that information brings to the business, allowing to stay one step of the threats and vulnerabilities that could compromise the way managers, and they have at hand a well-designed security policy firming commitment to confidentiality, integrity, availability, authenticity and legality.

Keywords: Security. Information Managers. IT. Vulnerabilities.

1 Introdução

O presente trabalho tem por objetivo apresentar como são realizadas, nas pequenas empresas, as tarefas pertinentes à segurança da informação e como elas são implementadas e administradas pelos seus gerentes ou responsáveis de TI.

A proposta é elaborada em tópicos que possibilitam mostrar os conceitos e as definições de segurança da informação, colocando definições e ideias sobre os princípios de segurança na informação, suas ameaças, vulnerabilidades e mecanismos de proteção à informação. Os gestores devem ser capacitados e ter pessoas capacitadas junto a mecanismos adequados à evolução na tecnologia.

A segurança da informação é, desde sempre, redutora de incertezas e, cada vez mais, transformadora de atitudes que tanto um indivíduo quanto uma organização podem tomar, dando a si um papel imprescindível no contexto socioeconômico da "era da informação".

2 Segurança da informação

O mundo virtual tem causado uma revolução notória em todos os aspectos, principalmente no mundo da comunicação. A internet se tornou um mecanismo que dissemina a informação em poucos segundos, tornando-a acessível em nível mundial, o que pode ser positivo ou negativo. Por isso existe a segurança da informação e suas medidas de controle e políticas de segurança, tendo como principal objetivo a proteção de informações de clientes e empresas. Essa evolução no meio tecnológico incentivou a fazer alterações de paradigmas, influenciando consideravelmente a forma como as empresas gerenciam seus negócios.

Os computadores tomam conta dos ambientes de escritório, rompem a barreira do acesso local à informação e chegam a qualquer lugar no mundo através dos, cada vez mais portáteis, *notebooks* e da rede mundial de computadores – a internet (SÊMOLA, 2003, p.3).

Como tudo evolui, a segurança da informação precisa estar sempre atenta a novos ataques, resguardando aquilo que é seu principal bem: a informação.

Os aspectos relativos a uma implementação eficiente de política de segurança da informação vêm evoluindo muito ao longo dos anos. Hoje, a segurança da informação requer políticas bem definidas, padrões, programas de conscientização, estratégias etc. Tudo aliado a *softwares* e *hardwares*, visando sempre à proteção daquilo que são os requisitos básicos – também chamado de C.I.D.A.L: confidencialidade, integridade, disponibilidade, autenticidade e legalidade, de acordo com a norma ISO 27002, que substitui a ISO 17799:2005 (código de boas práticas) –, ou seja, das vulnerabilidades que possam afetar o negócio de uma organização. Com elas sempre protegidas, a empresa estará apta a obter informações exatas a qualquer momento que desejar.

2.1 Ameaças

Elas sempre irão existir, porém, as vulnerabilidades podem ser controladas. Tratando-se de pessoas, podemos dizer que a principal preocupação está justamente na consciência dos responsáveis pela gerência da TI.

> Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio de exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade, disponibilidade, autenticidade e legalidade, consequentemente, causando impacto aos negócios de uma organização. (SÊMOLA, 2003, p.47)

Ameaças não faltam para um possível prejuízo à organização, sejam pessoas mal intencionadas ou um *software* não testado corretamente. Assim, elas são definidas por Sêmola (2003) como:

- **Naturais:** são aquelas decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades, poluição etc.
- **Involuntárias:** são inconscientes, quase sempre causadas pelo desconhecimento, podendo ser originadas de acidentes, erros, falta de energia etc.
- **Voluntárias:** são feitas propositadamente por agentes humanos, como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador.

Ainda podemos defini-las, segundo Shirey (2000), como:

- **Ameaça:** potencial violação de segurança. Existe quando houver uma circunstância, potencialidade, ação ou evento que possa romper a segurança e causar dano.
- **Ameaça de análise:** uma análise da probabilidade das ocorrências e das consequências de ações prejudiciais a um sistema.
- **Ameaça inteligente:** circunstância em que um adversário tem a potencialidade técnica e operacional para detectar e explorar a vulnerabilidade de um sistema.
- **Consequências de uma ameaça:** uma violação de segurança resultada da ação de uma ameaça. Inclui divulgação, usurpação, decepção e rompimento.

As ameaças sempre existirão e explorarão as vulnerabilidades, mas podem ser controladas. Existem vacinas para as externas, como os vírus; em outros casos, pode haver restrições a determinados lugares e programas, mas sem eliminação de 100% delas.

2.2 Proteção

A segurança, hoje, requer mais cuidado. Informação é a chave para qualquer organização projetar, traçar metas e planos a fim de estar sempre apta à forte concorrência no mercado.

> A política de segurança é um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico, gerencial e pelos usuários internos ou externos. Pode ser usada para definir

> as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais. (DIAS, 2000)

A política de segurança é uma formalização de todos os aspectos importantes da organização para a proteção e o controle de seus recursos computacionais, dando um respaldo importante às proteções física e lógica.

A segurança física tem como objetivo proteger equipamentos e informações contra usuários não autorizados, prevenindo, assim, o acesso a esses recursos. Ela deve se basear em perímetros pré-definidos nas imediações dos recursos computacionais. Já a segurança lógica é a forma como um sistema é protegido no nível operacional e de aplicação.

Existe ainda algo que é de suma importância para um negócio, o PCN – Plano de Continuidade de Negócio. Trata-se de uma forma independente da política de segurança, objetivando agir no menor tempo possível e de acordo com as prioridades da organização após a ocorrência de algum desastre na segurança.

> Convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio NBR ISSO/IEC 17799. (2005, p.14)

Para tanto, colocamos que a segurança da informação está baseada em três pilares: pessoas, processos e tecnologia. Ter *softwares* adequados, pessoas treinadas e com o senso voltado para o negócio da empresa não somente será benéfico para a organização, mas para toda a equipe centrada no negócio.

O site <www.cert.br> "mostrou que o número total de notificações de incidentes no primeiro trimestre de 2011 foi ligeiramente inferior a 91 mil, o que corresponde a um aumento de quase 118% em relação ao trimestre anterior e de 220% em relação ao mesmo período de 2010". Mesmo tendo uma queda em nível nacional, é algo preocupante para os gestores de TI.

Tempos na tabela abaixo exemplos de ataques.

FIGURA 2: Tipos de ataques

Descrição das categorias de incidentes reportados ao *site* cert.br:	
Worm	Notificações de atividades maliciosas relacionadas ao processo automatizado de propagação de códigos maliciosos na rede.
DoS	DoS (*Denial of Service*): notificações de ataques de negação de serviço, nas quais o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, um computador ou uma rede.
Invasão	Um ataque bem sucedido que resulte no acesso não autorizado a um computador ou uma rede.
Web	Um caso particular de ataque visando especificamente o comprometimento de servidores *web* ou desfigurações de páginas na internet
Sem	Notificações de varreduras em redes de computadores com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
Fraude	Segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Essa categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes nos quais ocorre uma tentativa de obter vantagem.

Fonte: CERT.BR (2011)

Vale lembrar que não se deve confundir *scan* com *scam*. *Scam* são quaisquer esquemas para enganar um usuário, geralmente, com finalidade de obter vantagens financeiras. Ataques desse tipo são enquadrados na categoria "fraude".

Segue, na figura abaixo, um gráfico mostrando as estatísticas de incidentes desde 1999.

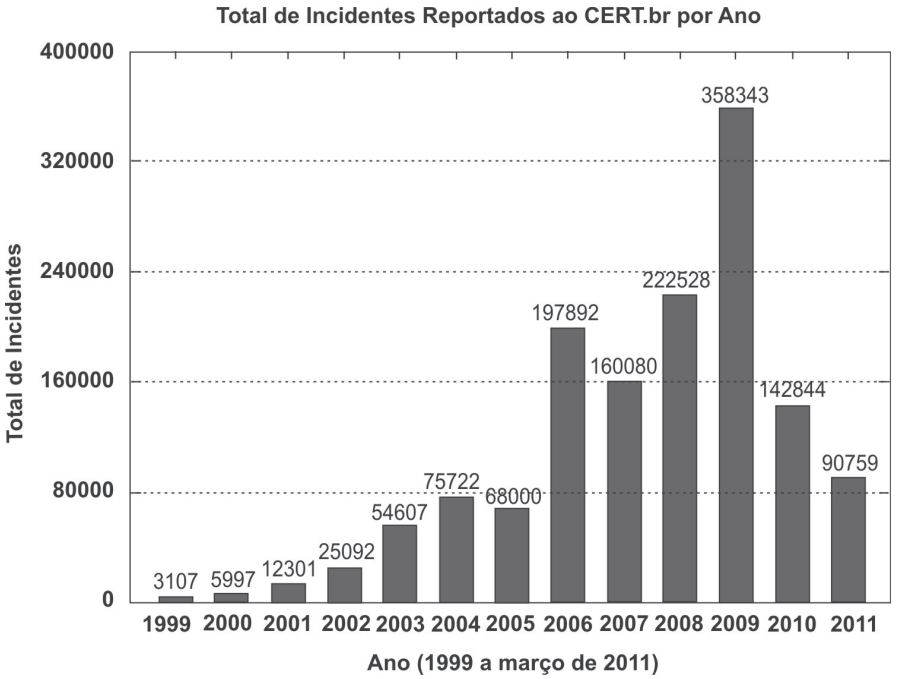

Figura 1: Incidentes reportados
Fonte: CERT.BR (2011)

2.3 Riscos

Uma das primeiras normas definidas foi a BS7799 – *Code of Practice for Information Security Management*, em dezembro de 2000, que ganhou padrão internacional ISSO/IEX 17799:2000, permitindo às empresas investir em segurança, focando sempre o C.I.D.A.L, com 127 controles de segurança bem definidos para o ambiente em nível de gerência de segurança, englobando controles de segurança para implementação e administração de sistemas e redes, guias para implantação de políticas de segurança, planos de continuidade de negócio e aderência à legislação.

Entender as vulnerabilidades ou os riscos que a organização corre possibilita que a empresa elabore sua política de segurança de uma forma que sempre se fortaleça, primando, assim, pelas C.I.D.A.L. Segundo Sêmola (2003, p.50), risco é "probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade, disponibilidade, autenticidade e legalidade, causando, possivelmente, impactos nos negócios."

Uma análise de riscos bem elaborada pode somar ideias desde os passos menos visíveis, tornando-a mais eficaz e estabelecendo prioridades nos investimentos. Isso se tratando de segurança física. Para complementar essa análise, temos o controle de acesso, em que o objetivo é controlar o acesso à informação. Como não existe a perfeição em medidas de prevenção, torna-se necessário que falhas de segurança sejam identificadas e possam ser tomadas ações para reduzir seu impacto.

A medida mais acessível e mais comum é o *login* e o *password*, através dos quais são informados o nome do usuário e sua autenticação ou senha. Um problema recorrente são as fracas senhas, aquelas que não são tão complicadas para se descobrir. Por isso, sempre são recomendadas senhas com oito caracteres, com números, letras e caracteres especiais.

Portanto, a empresa deve dar suma importância àquilo que é seu maior ativo, a informação. Assim sendo, ela terá sempre a organização e a disponibilidade daquilo que precisa, caso prime pela sua segurança.

2.4 Processos de segurança

A segurança é um processo que se deve ter ou se adaptar a ele, e se resume basicamente em avaliação, análise e síntese. Ele deve ser feito continuamente, para que possa sempre trabalhar em cima do resultado, seja negativo ou positivo. Além das etapas de planejamento, padronização e documentação, podemos mencionar:

- *Plan* – Definição das metas.
- *Do* – Execução do planejado consoante as metas e métodos pré-definidos.
- *Check* – Análise dos resultados obtidos, conferindo se o que foi desenvolvido está dentro do que foi traçado.
- *Action* – Verificação dos resultados, fazendo as devidas correções a fim de melhorar o processo.

Em uma política de segurança de informação, devem-se elaborar princípios sobre como a organização irá se proteger, controlar e monitorar seus recursos computacionais. Três processos são definidos: nível estratégico, nível tático e nível operacional. Descrevemos abaixo cada um deles.

2.4.1 Nível estratégico

Trata-se de uma tomada de decisão rápida, que ocorre eventualmente e exige segurança e bom senso para que não torne o trabalho vulnerável e comprometa o que vem sendo feito.

2.4.2 Nível tático

Engloba uma padronização a ser seguida pela empresa, seja de *softwares* ou equipamentos, estabelecendo o mesmo nível de segurança para toda a organização, não deixando um setor ou uma filial destoar.

2.4.3 Nível operacional

Dá continuidade ao que foi dito antes, com uma documentação detalhando tudo a ser seguido, tornando a parte operacional adequada, de forma que fique fácil manuseá-la, pois esses trabalhos são realizados por pessoas e cada uma tem um modo de pensar e agir. Com isso, estabelecem-se, de forma documental, regras a serem seguidas.

3 Conclusão

A segurança da informação vem sendo mais trabalhada nas organizações, devido às tentativas de invasão a que estão sujeitas em nosso mundo globalizado. E como o maior patrimônio delas é a informação, é necessário ter um cuidado maior, pois esta está cada vez mais à disposição no mundo virtual.

Nos últimos tempos, a tecnologia da informação evoluiu muito, fortalecendo o uso de mecanismos de segurança para a sobrevivência e competitividade das organizações.

Hoje, quase todos os computadores estão conectados à internet, fazendo com que qualquer informação no mundo virtual corra rapidamente e se torne alvo para pessoas com más intenções, não descartando incidentes que possam ocorrer, como acidentes naturais. Portanto, não há segurança absoluta, mas pontos vulneráveis podem ser controlados de maneira eficaz se forem analisados de forma contínua, com o objetivo de reduzir ao máximo esses riscos, mantendo o ciclo da informação sempre preservado.

Referências

DIAS, Cláudia. *Segurança e auditoria da tecnologia da informação*. Rio de Janeiro: Axcel Books, 2000.

ESTATÍSTICAS e incidentes reportados ao CERT.br: janeiro a março de 2011: análise de alguns fatos de interesse observados neste período. Disponível em: <http://www.cert.br/stats/incidentes/2011-jan-mar/analise.html>. Acesso em: 11 maio 2011.

SÊMOLA, M. *Gestão da segurança da informação*. Rio de Janeiro: Campus, 2003.

SHIREY, R. RFC 2828: Internet Security Glossary. *The Internet Society*, 2000. Disponível em: <http://www.ietf.org/rfc/rfc2828.txt?number=2828>. Acesso em: 11 maio 2011.