Revista Eletrônica em Gestão e Tecnologia
Print ISSN 2316-4972
ONLINE 2447-0422
FAQI
FACULDADE QI BRASIL

SEGURANÇA DA INFORMAÇÃO

João Paulo de Oliveira Troxinski

troxinski.joao@gmail.com

Fundamentos de banco de dados – Silvio Cesar Viegas.

Resumo

Este artigo tratará sobre a importância de se manter as informações de empresas seguras, livres de riscos e perigos que possam danificá-la. Identificando os pontos de risco e boas condutas que podem aumentar o nível de segurança para seus e obter maior proteção contra invasões e vazamentos de informações, obtendo assim uma resposta à pergunta. Qual a importância de manter a segurança de suas informações? E como obter melhor proteção?

Palavras-chave: Segurança da informação, proteção de dados, ameaças.

Introdução

Vazamento de informações não ocorrem somente por meio de espionagem. Diariamente, redes de computadores e hosts são invadidos, e a maioria destes ataques acontecem por códigos secretos fracos, porém a cada dia surgem novas técnicas de invasão que podem ser de diversas naturezas tornando-se assim muito mais difícil de descobrir. Porém pode acontecem vazamentos por meio de funcionários, que não possuem uma preparação adequada ou estão insatisfeitos com a empresa. As vezes um simples vazamento pode trazer muitos prejuízos financeiros ou perda de confiança por parte do público, e nisto a mídia tem uma grande parcela de responsabilidade, adotando a não vinculação de notícias duvidosas. Segundo pesquisas divulgadas pela Symantec, empresa especializada em segurança da informação 62% dos profissionais vazam dados sigilosos das empresas. (CANEPA 2013).

1 Ameaça

O conceito de ameaça consiste em possível violação de um sistema computacional e pode ser acidental ou intencional. A ameaça acidenta não e planejada pode ser uma falha no sistema. Já a intencional e feita com premeditação intencional pode ser desde um acesso não autorizado no sistema até ataques muito mais sofisticados como por exemplo os ataques realizados por hackers.

2 Sistema e suas vulnerabilidades

Após compreender o sistema de informação como um conjunto de elementos ou componentes inter-relacionados, que coletam (entrada), manipulam (processamento) e disseminam (saída) os dados e a informação fornecem um mecanismo de feedback para atender um objetivo. (DANTAS 2011). Figura 01

Revista Eletrônica em Gestão e Tecnologia
Print ISSN 2316-4972
ONLINE 2447-0422
FAQI
FACULDADE QI BRASIL

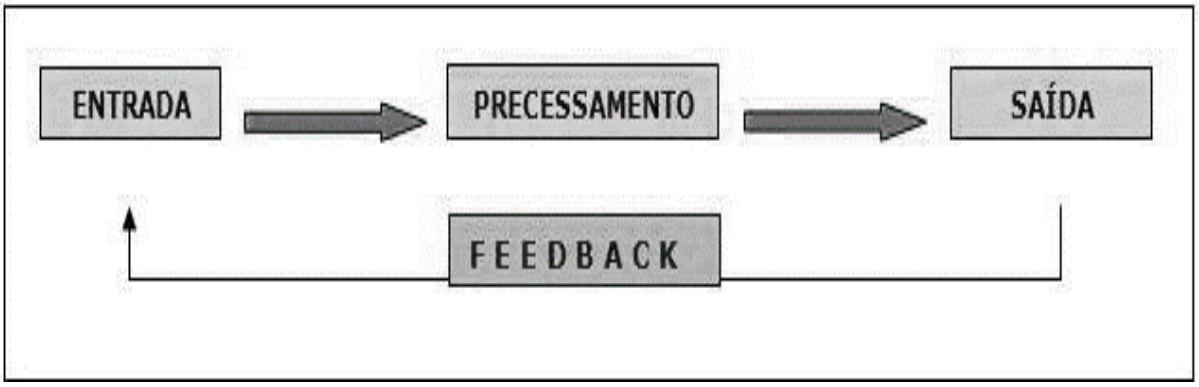

Figura1: Componentes de um sistema de informação.

Fonte: DANTAS 2011

A três fatores que podem oferecer riscos a um sistema, onde o risco é compreendido como algo que cria oportunidades ou produz perdas. Com relação à segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. (DANTAS 2011)

- Sistemas na internet: Podem trazer indisponibilidade de serviços, furtos de dados, perda da privacidade, perda financeira, danos à imagem e perda de confiança na tecnologia.
- Ataques: O sistema pode sofrer ataques por meio de vândalos, governo, criminosos ou espionagem industrial.
- Vulnerabilidade: Pode haver danos através de defeitos de software, falhas de configuração, uso inadequado, fraquezas advindas da complexidade dos sistemas. (HOEPERS 2014)

Os ataques ocorrem através do uso ou acesso não autorizado de um serviço, computador ou rede. Um programa ou parte de um programa pode explorar o sistema e verificar sua vulnerabilidade, e assim podendo causar danos ao sistema. (HOEPERS 2014)

Normalmente os ataques através da internet o usuário recebe um documento por e-mail, com uma identificação comum, exemplo ata de reunião, quando este arquivo e aberto por um programa vulnerável, o conteúdo malicioso explora a vulnerabilidade, este código e executado no computador baixando e executando um malware (do inglês MALicious software. Trata-se de um software destinado a se infiltrar em um computador alheio de forma ilícita, cavalo de Troia e spyware.) Ele se conecta a um servidor de comando e controle onde recebe comandos para atacar.

Entre os ataques estão:

- Instalar spyware.
- Enviar spam.
- Atacar outras redes.
- Enviar e-mails com conteúdos maliciosos.

Quando os ataques são contra servidores na web, é instalado ferramentas em um site já comprometido, que fica à procura de sites, constrói uma lista de sites a serem atacados e em cada site realiza um ataque em logins e senhas, quando obtêm acesso ao site pode causar:

- Alterar seu conteúdo.
- Levantar páginas de phishing ("pescaria", tem o objetivo de “pescar” informações e dados pessoais importantes).

- Inserir scripts que exploram a vulnerabilidade de navegadores dos visitantes, com o objetivo de infectar os usuários. (HOEPERS 2014)

Todos estes ataques podem resultar em danos para o sistema, no caso de uma empresa pode perder credibilidade, dinheiro ou segredos o qual pode trazer muitas consequências. Muitas empresas não investem em segurança, talvez por pensar ser um custo desnecessário ou até mesmo um investimento sem retorno, porém quando a uma quebra de segurança, quando arquivos confidenciais são expostos, o prejuízo pede chegar a levar estas empresas a pagar indenizações, perder segredos de processo, receitas de fabricação e dados pessoais. (KUROSE 2010)

3 Como proteger seu sistema

Grande parte da vulnerabilidade está na falta de treinamento dos funcionários ou falta de conhecimento por parte do usuário. "A conscientização deve ser parte integrante do treinamento de segurança das empresas". (CANEPA 2013).

Segundo, Hoeprsh, 2014, uma forma de garantir a segurança, é se certificar que os recursos só sejam conhecidos por funcionário que tenham permissão para usá-lo, através dê conta de usuário, conta de banco e e-mail, e verificando se a identificação e de quem realmente está acessando através de biometria, token e senhas, e também ter níveis de acesso no sistema onde sua permissão vá até o ponto onde e autorizado.

É muito difícil conseguir ter um sistema 100% seguro, assim para conseguir atingir um nível razoável de segurança em seu sistema, tem alguns objetivos a serem atingidos: Conter o mais rápido possível as ameaças, recuperar e mitigar e, adaptar-se ao senário e as mudanças rapidamente e fazer com que seu sistema continuei funcionando mesmo na presença de ataques ou falhas. Para estar preparado existem etapas a serem feitas: Devesse identificar o que é crítico e precisa ser protegido definindo políticas de uso, acesso e segurança realizando isso através de profissionais que estejam preparados para treinarem e conscientizar os usuários sobre os riscos e medidas de segurança. (HOEPERS 2014). Porém apenas a existência de uma política não resolve, é preciso ter rigor e fiscalização. Com a implementação de tecnologias de monitoramento e notificar automaticamente os funcionários sobre violações. Essas medidas podem aumentar a conscientização dos funcionários e impedir roubos.

3.1 Política de Segurança da Informação

As políticas da informação são instruções claras para como o empregado deve se comportar para guardar informações, e é uma arma fundamental para contra-atacar possíveis ameaças à segurança. Ele é implementada através de treinamento de seus operadores com procedimentos bem documentados, porém deve-se estar atento, pois mesmo com uma política bem implantada não impede que seu sistema seja invadido, porem o objetivo deves ser minimizar os danos até que os riscos estejam em um nível aceitável. (FONSECA, 2009).

Para obter recuperação de dados, sempre ter uma cópia, um backup que deve sempre estar atualizado. Existem aplicativos que proporcionam uma rápida recuperação dos backups em caso de perda dos originais do sistema.

4 Conclusão

Após o a análise deste artigo conclui-se que a falta de segurança da informação, ocorre por vários motivos, na maioria das vezes pode ocorrer por falha do operador do sistema, que por negligência, descuido, problemas pessoais, problemas com a empresa pode negligenciar.

Outro motivo em muitos casos é por falta de um treinamento adequado da parte da empresa para com os operadores do sistema. Isso acaba gerando vários transtornos, pois um operador mal treinado pode inevitavelmente deixar que informações fiquem desprotegidas, isso gerando roubo de informação ou um vazamento, com danos muitas vezes irreparáveis para e empresa ou instituição para qual ele presta serviço.

A segurança é um simples produto ao qual é possível adquirir. Ela é adquirida, aplicada em seu sistema e esquecida na maioria das vezes, na segurança deve sempre haver um processo de evolução contínua, que abranja todas as áreas desde a alta direção de uma empresa até os usuários que executam operações cotidianas devendo ser encarada como uma forma de aumentar os níveis de confiança internos e externos. Pois grande parte do sucesso de uma empresa depende de sua confiabilidade.

Referência

CANEPA, Lana, especial para a Gazeta do Povo, gazeta do povo, 02/07/2013, disponível em<http://www.gazetadopovo.com.br/economia/62-dos-profissionais-vazam-dados-sigilosos-das-empresas-bgpop4f9gqwm4xpi0qc6299ou> acesso em 18/09/2017.

CHESWICK, William R. Firewalls e segurança na internet: Repelindo o hacker ardiloso, 2° edição. Porto Alegre. 2005.

FONSECA, Paula Fernandes. Gestão de Segurança da Informação: O Fator Humano. Curitiba. 2009. Disponível em <https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS08A/Paula%20Fernanda%20Fonseca%20-%20Artigo.pdf> Acesso em 26 set 2017

KUROSE, James. Redes de computadores e internet: 5° edição, uma abordagem top donw. São Paulo. 2010.

HOEPERS, Cristine. Fundamentos de Segurança da Informação. EGI escola de governança da internet no Brasil, Santa Catarina, 2014. Disponível em: < www.cert.br/docs/palestras/certbr-egi2014.pdf>. Acesso em: 10 set.2017.

NETO, Abner da Silva. XXX conferencia ANPAD: Gestão da Segurança da Informação: fatores que influenciam sua adoção em pequenas e médias empresas. Rio de Janeiro 2007. Disponível em <http://www.anpad.org.br/admin/pdf/ADI-B3180.pdf>. Acesso em 11 set 2017.

PINHEIRO, Jose Maurício dos santos. Ameaças e ataques aos sistemas de informação: prevenir e antecipar. 2005. Disponível em: < Acesso em: 10 set.2017 > Acesso em: 19 set.2017.