SEGURANÇA DA INFORMAÇÃO NAS REDES CORPORATIVAS

Ricardo de Melo Justi[1], Luís Augusto Mattos Mendes (Orientador)[1]

[1]Departamento de Ciência da Computação – Universidade Presidente Antônio Carlos (UNIPAC)
Campus Magnus – Barbacena – MG – Brasil

rickjusti@yahoo.com.br**,** luisaugustomendes@yahoo.com.br

Resumo. Como a informação é fundamental para as empresas e as mesmas têm a necessidade de trocar informações, é importantíssimo estar atualizado as novas ameaças e métodos de ataque que surgem diariamente, pois no envio de uma informação, ela pode ser interceptada, ou seja, terceiros também saberão o conteúdo daquela informação. Como conseqüência deste ato, informações sigilosas estarão em mãos erradas. A Segurança da Informação visa auxiliar na confidencialidade e na integridade da informação, para que informações sigilosas não sejam roubadas ou caiam em mãos erradas. No decorrer do trabalho será abordado a política de segurança, ataques e ameaças mais freqüentes, métodos de proteção, segurança física e pontos falhos que ocorrem nas empresas.

Palavras-Chave: Redes; Segurança da Informação.

1. Introdução

Atualmente, com o grande crescimento do uso de computadores em ambientes corporativos e com a necessidade de trocar informações, manter os dados bem protegidos é essencial, pois a informação é fundamental para as corporativas. Corporativa no caso é a organização (conjunto de empresas pertencentes à mesma organização) nos quais os usuários trabalham e usufruem dos dados da mesma para desenvolver e concluir suas atividades e que será nomeada assim durante o trabalho.

As corporativas necessitam de um ambiente onde a troca de informações possa ser feita de uma maneira segura, rápida e restrita a redes externas, ou seja, para manter essas informações sob segurança é importante relevar os perigos que percorrem a rede e estar atento a qualquer risco tanto humano quanto tecnológico.

Portanto, a Segurança da Informação visa proteger os dados importantes dos computadores e os arquivos sigilosos armazenados, pois com a perda ou modificação dos mesmos, a corporativa terá prejuízos drásticos[1].

No decorrer do artigo, a seção 2 falará sobre o conceito de segurança da informação e seus principais objetivos. Falará também sobre política de segurança, os métodos mais comuns de ataques e ameaças, métodos de proteção e segurança física da informação. Na seção 3 falaremos sobre os pontos falhos da corporativa, onde usuários sem treinamentos adequados e profissionais de informática irresponsáveis colocam a corporativa em risco. Demais pontos falhos que serão abordados: senhas fracas, falhas em *backups* e falhas no sistema de log.

2. Segurança da Informação

Hoje em dia, com as crescentes perdas de dados aliados a ataques e roubos, é extremamente necessária a utilização de ferramentas em prol do sigilo e integridade dos mesmos.

No entanto, a segurança da informação que visa proteger as informações disponíveis em uma rede que não podem ser acessadas por pessoas não-autorizadas, ou seja, deve incluir uma garantia de privacidade, onde tende a minimizar as vulnerabilidades de acessos indevidos às informações (dados) confidenciais. A expectativa é que os dados estejam sempre disponibilizados quando for solicitado, seguros contra acessos não autorizados e corretos sem modificações indevidas[1].

Alguns de seus objetivos são:

- Confidencialidade – A definição clássica de confidencialidade é a garantia do resguardo das informações dadas pessoalmente em confiança e a proteção contra a sua revelação não autorizada. Atualmente, confidencialidade é considerada como sendo o dever de resguardar todas as informações que dizem respeito a uma pessoa, isto é, a sua privacidade. A confidencialidade é o dever que inclui a preservação das informações privadas e íntimas[1].
- Criptografia – Consiste em cifrar um arquivo ou mensagem usando um conjunto de cálculos. O arquivo cifrado (ou encriptado) torna-se incompreensível até que seja desencriptado[1]. Os cálculos usados para encriptar ou desencriptar o arquivo são chamados de chaves. Apenas quem tiver a chave poderá ler o arquivo. Existem basicamente dois sistemas de uso de chaves. No primeiro (simétrico) são usadas chaves simétricas, onde as duas partes possuem a mesma chave, usada tanto para encriptar quanto para desencriptar os arquivos. No segundo sistema (assimétrico) temos o uso de duas chaves diferentes, chamadas de chave pública e chave privada. A chave pública serve apenas para encriptar os dados e pode ser livremente distribuída, a chave privada permite desencriptar os dados.
- Controle de Acesso - visa ter um controle dos usuários que estão acessando ou modificando as informações. Através do login, poderemos ter a hora e sua identificação para termos certeza de saber quem fez algo (intencionalmente ou não) de errado[2];
- Disponibilidade – o dado deve estar disponível sempre que for solicitado pelo usuário. Exemplo: Acidentalmente um usuário apagou uma planilha essencial de seu trabalho. A solução para este caso é ter este dado em backup para que ele possa ter imediatamente a planilha restaurada e prosseguir no seu trabalho[2];

- Integridade – a informação deve ser mantida como o proprietário da informação a disponibilizou, evitando que ela seja modificada ou apagada;
- Não repúdio – maneira de um destinatário provar que realmente recebeu a mensagem de uma determinada origem, mesmo que está origem negue que enviou a mensagem[2].

2.1 Política de Segurança

> *"Uma política de segurança é a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa. Tem como propósito informar aos usuários, equipe e gerentes, as suas obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados. Oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos. Para que uma política de segurança se torne apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de empregados dentro da corporativa. É especialmente importante que a gerência corporativa suporte de forma completa o processo da política de segurança, caso contrário haverá pouca chance que ela tenha o impacto desejado[3]."*

Através dela, é definido o que será protegido, quais as ferramentas de combate a ataques e ameaças serão usadas e o custo da implementação destas ferramentas. Também tem como objetivo educar o usuário, ensinando-lhe procedimentos que tornem as suas ações seguras, evitando provocar riscos a corporativa.

2.2 Ataques e Ameaças

Atualmente as ameaças e os ataques estão muito poderosos, trazendo inúmeros malefícios para as empresas, como perdas sigilosas de informações e também perdas financeiramente consideráveis. "As ameaças podem ser classificadas como acidentais ou intencionais, podendo ambas serem ativas ou passivas. Ameaças acidentais são as que não estão associadas à intenção premeditada. As ameaças intencionais variam desde a observação de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema[3]." O ataque define-se por usuários que utilizam recursos computacionais de maneira ilícita. Alguns tipos de ataques são:

- Programas de Varredura – são softwares que percorrem a rede testando máquinas remotas a fim de identificar os sistemas operacionais que elas executam e exigem a identificação do usuário[3]. Um conhecido programa é o NESSUS. O NESSUS é uma ferramenta de auditoria

muito usada para detectar e corrigir vulnerabilidades nos computadores da rede local. Ele realiza uma varredura de portas, detectando servidores ativos e simulando invasões para detectar vulnerabilidades.

- Ataques DoS (*Denial of Service*) – O ataque de negação de serviço torna um servidor inoperante sobrecarregando-o excessivamente com solicitações de serviço. Nesse tipo de ataque é feita uma sobrecarga de pacotes, formando uma quantidade de dados maior que uma rede ou *host* possa agüentar tornando a rede instável.
- Ataques DDoS - São ataques semelhantes ao DoS, tendo como origem diversos e até milhares de pontos disparando ataques DoS para um ou mais sites determinados[3]. Para isto, o invasor coloca agentes para dispararem o ataque em uma ou mais vítimas. As vítimas são máquinas escolhidas pelo invasor por possuírem alguma vulnerabilidade. Estes agentes, ao serem executados, se transformam em um ataque DoS de grande escala.
- Cavalos de Tróia – "é um programa que aparenta ter uma função útil, mas possui alguma função maliciosa que burla os mecanismos de segurança. Não possui a capacidade de se auto replicar. Como exemplo pode-se citar um jogo puxado pela Internet, que na verdade, ao ser executado, tira a atenção do usuário enquanto executa algum dano ao computador ou seus dados em segundo plano[3];"
- Quebra de Senhas - Para acessar algo é necessário uma senha de acesso, muitos invasores tentam quebrar estas senhas através de técnicas de quebras de senhas, como tentar as senhas padrões de sistemas ou as senhas simples como nomes pessoais, nome da empresa, datas, entre outros[3]. Mas para facilitar a descoberta da senha, existem diversos programas, como dicionários de senhas e programas que tentam todas as combinações possíveis de caracteres para descobrir a senha.
- *Spoofing* - Nesta técnica, o invasor convence alguém de que ele é algo ou alguém que não é, sem ter permissão para isso, conseguindo autenticação para acessar o que não deveria ter acesso, falsificando seu endereço de origem[3]. É uma técnica de ataque contra a autenticidade, onde um usuário externo se faz passar por um usuário ou computador interno.
- *Sniffer* - é um programa de computador que monitora passivamente o tráfego de rede, ele pode ser utilizado legitimamente, pelo administrador do sistema para verificar problemas de rede ou pode ser usado ilegitimamente por um intruso, para roubar nomes de usuários e senhas. Este tipo de programa explora o fato dos pacotes das aplicações TCP/IP não serem criptografados. Entretanto, para utilizar o *sniffer*, é necessário que ele esteja instalado em um ponto da rede, onde passe tráfego de pacotes de interesse para o invasor ou administrador.
- Vírus – são códigos com objetivos de se agregar a códigos de outros programas a fim de infectá-los, causando danos leves e irreparáveis. Modifica os outros programas, introduzindo cópias, eventualmente alteradas deles próprios[3]. Podem causar perda de dados, ou ainda, alterar o funcionamento normal do sistema. Alguns tipos de vírus atacam também a privacidade dos sistemas. A seguir alguns tipos de vírus:

- Vírus simples: é definido como sendo um software com capacidade de se duplicar, infectando outros programas, usualmente com alguma intenção maliciosa. Um vírus não pode executar-se sozinho, requer que o seu programa hospedeiro seja executado para ativar o vírus[3];

- *"worm* ou "verme": definido como sendo um programa de computador que pode se executar independentemente, propagar-se pelos computadores de uma rede sozinho, podendo consumir os recursos dos computadores destrutivamente[3];"

- "Vírus polimorfo: tipo de vírus que modifica a si mesmo à medida que se dissemina, dificultando a sua localização e eliminação[3];"

- "Vírus de Macro: utiliza-se da linguagem VBScript dos softwares Microsoft e pode ser executado em qualquer computador que possua, por exemplo, o aplicativo Word instalado[3]."

- *Backdoors* – são portas abertas que administradores esquecem de desativar, assim o sistema fica aberto a quem quiser entrar. São abertos devido à falhas dos programas, podendo ocorrer acidentalmente ou não[3].
- *Trapdoor* – ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando ou a um evento, ou seqüência de eventos predeterminados[3].

2.3 Métodos de Proteção

Para evitar os ataques, invasões e conseqüentemente às perdas de informações, adiante estarão as medidas para que não ocorram malefícios com as informações.

- Firewall – tem como objetivo isolar uma rede local de acessos não autorizados[4]. Fica localizado entre a rede local e a internet, gerenciando as informações que entram e saem da corporativa. Existem dois tipos de firewall: o filtro de pacotes de rede e o proxy. O filtro de pacotes, mediante a configuração, determina que pacote possa ser colocado na rede interna e que pacote deve ser filtrado. Já o proxy, não permite que nenhuma máquina de rede interna faça conexões externas diretamente. Com a utilização do firewall, pode-se estabelecer filtros complexos como filtrar e-mails com anexos EXE e DOC, que contém maiores chances de vírus.
- Detector de Intrusão (IDS) – o *Intrusion Detection System* é equivalente a um alarme contra potenciais ameaças externas e permitem detectar eventuais entradas ilícitas na rede das corporativas[4]. O detector de intrusão monitora e relata atividades maliciosas como: ataques

de negação de serviço (DoS), worms, trojans e vírus. É bom lembrar que o IDS não substitui o firewall, mas sim complementa-o.

- Criptografia – Como dito antes a criptografia tem como objetivo garantir o sigilo e a integridade da informação[4]. Ela é feita da seguinte maneira: o remetente cifra a mensagem original aplicando um algoritmo de ciframento, com auxílio da chave privada conhecida também pelo destinatário, obtendo assim a mensagem cifrada. Logo, a mensagem cifrada é enviada ao destinatário. Quando o destinatário receber a mensagem, aplica-se um algoritmo de deciframento, utilizando à mesma chave privada. Ferramentas de criptografia: RSA, DES, AES.
- Antivírus – Os antivírus possuem uma base de dados com os códigos dos vírus mais conhecidos. Faz-se necessário mantê-lo sempre atualizado para que o antivírus possa estar sempre detectando uma possível ameaça[4]. "Um detalhe que deve ser analisado cuidadosamente é a provável perda de desempenho dos computadores pela ação constante do antivírus, visto que é um programa que pode ser configurado para se procurar, em todos os arquivos utilizados a cada momento, assinaturas de vírus. Esse processo de procura utiliza os recursos do computador. Pode-se configurar o software de antivírus para verificar apenas os arquivos novos, criados por um programa ou baixados da Internet. Nesse tipo de configuração, é recomendado que na primeira inicialização do computador, o software verifique todos os arquivos armazenado a procura de vírus[4]."
- Controle de Acesso – o sistema tem que prever cada *login* de cada usuário, a hora, e sua identificação para ter conhecimento se, por acaso, alguém danificou um arquivo para descobrir e repreender o usuário.
- *Backup* – ponto importantíssimo para qualquer corporativa. O backup garante a segurança e a disponibilidade dos dados da corporativa[4]. É necessário definir o tipo de mídia de armazenamento de dados que será utilizada. Existem fitas magnéticas, discos óticos e web *backup*, onde as empresas fornecedoras ficam com a responsabilidade de fazer os *backups*. Alguns tipos de *backups*:
  - *Backup Full* - Consiste no *backup* de todos os arquivos. Sua desvantagem é que se alguns arquivos forem modificados, não é verificado se o arquivo foi alterado desde o último backup, então é feito um backup de tudo indiscriminadamente para a mídia do mesmo, tendo modificações ou não.

  - *Backup Incremental* - Os *backups* incrementais primeiramente fazem uma verificação se o horário de alteração de um arquivo é mais recente que o horário de seu último. Se não for, o arquivo não foi modificado desde o último backup e pode ser ignorado desta vez. A vantagem principal em usar *backups* incrementais é que rodam mais rápido que os *backups* completos. A principal desvantagem dos *backups* incrementais é que para restaurar um determinado arquivo, pode ser necessário procurar em um ou mais *backups* incrementais até encontrar o arquivo.

- *Backup Diferenciado* - *Backups* diferenciais são similares aos *backups* incrementais, pois ambos podem fazer backup somente de arquivos modificados. No entanto, os *backups* diferenciais são cumulativos, em outras palavras, no caso de um backup diferencial, uma vez que um arquivo foi modificado, este continua a ser incluído em todos os *backups* diferenciais. Isto significa que cada *backup* diferencial contém todos os arquivos modificados desde o último backup completo, possibilitando executar uma restauração completa somente com o último backup completo e o último backup diferencial.

2.4 Segurança Física

A segurança física é muito importante para segurança dos dados também. Após definir a política de segurança, fica então determinado o que será protegido e como será protegido. É de extrema importância fazer com que os CPD[1]'s estejam fortemente seguros. Os CPD[1]'s devem estar longe de materiais combustíveis, tubulações de água e esgoto, antenas de telecomunicações e estações de energia elétrica. Deve conter também porta(s) corta fogo. Recomenda-se que a energia elétrica seja fornecida por *no-breaks* e fazer instalação de um gerador, pois caso falte energia externa, a sala do CPD[1] estará alimentada.

No CPD[1], deve conter[5]:

- Sistema anti-incêndio - para que num possível incêndio não ocorra a perda dos dados;
- Refrigeração na sala - muito recomendável ter ar-condicionado para que o CPD[1] tenha um controle de temperatura e umidade em torno de 22º C;
- Câmeras de Vigilância - estas filmagens devem ser gravadas e armazenadas para consultas futuras. É recomendado ter vigilância constante tanto internamente quanto no perímetro externo, configurando para que o alarme seja acionado com detecção de movimentos;
- Controle de Acesso – o CPD[1] deve contar um sistema de controle eletrônico com mais de um nível de segurança, como por exemplo, cartão magnético e senha de acesso. Identificações como impressões digitais e íris são bem recomendadas.

3. Pontos Falhos

Com certeza, os maiores fatores de problemas na corporativa, não são os programas e as regras determinadas para uma melhor segurança na empresa, mas sim, o usuário e os profissionais da área de informática irresponsáveis. Pois sem treinamento, o usuário que não sabe proceder bem com computador com certeza trará problemas, como abrindo e-mails de falsas entidades como bancos e a receita federal. Já o profissional despreparado, deixa sua máquina ao descaso enquanto vai tomar

[1] CPD – Centro de Processamento de Dados que visa auxiliar nos dados administrativos e no processamento de dados da corporativa[5].

um café, mesmo sabendo que alguém pode aproveitar da situação e copiar dados importantes em seu nome, causando até sua demissão da corporação. Para evitar tais conseqüências, é recomendável fazer um treinamento com o usuário e uma reciclagem dos profissionais despreparados de acordo com a norma da política de segurança da corporativa. A seguir falaremos sobre alguns pontos falhos que ocorrem nas corporativas.

3.1 Senhas fracas

As senhas de um usuário podem ser facilmente descobertas, porque na maioria das vezes o usuário utiliza senhas de fácil recordação, como: nome, sobrenome, data de aniversário, nome da esposa, nome(s) do(s) filho(s), dentre outros. Além do problema citado anteriormente, existem também os demais:

- Usuários frequentemente passam suas senhas para amigos, sem saber o risco que ele está correndo ao se fazer o devido ato;
- Guardam senhas em programas como MS-Word e MS-Excel;
- Anotam suas senhas em papéis e deixam à amostra para todos.

Para evitar tais problemas, é necessário fazer um treinamento com os usuários da corporativa, ensinando-lhes maneiras de sigilo e senhas fortes evitando assim conseqüências como perda de dados importantes.

Senhas fortes são constituídas em uma mesclagem de letras maiúsculas e minúsculas, e de caracteres (!@#$$?), com no mínimo oito dígitos. É recomendado fazer a substituição da mesma em um intervalo de dois meses, evitando repetir senhas anteriores.

3.2 Backups falhos

As corporativas realizam *backups* diários, mas infelizmente em alguns casos, os responsáveis pelo gerenciamento dos *backups* não se preocupam em realizar testes, para confirmar se o backup do correspondente dia foi feito com sucesso. Às vezes o backup diário não é feito por algum erro, assim os arquivos não são salvos, ou seja, não houve backup deste dia, provocando sérios riscos, pois se a corporativa necessitar de um arquivo deste dia, não o terá, causando assim sérios problemas. Geralmente, uma atualização diária é pouco diante das necessidades da empresa, caso venha a sofrer algum dano. É recomendável também fazer um *backup* mensal, pois se por algum evento, a corporativa necessitar de dados passados, certamente os terá no backup mensal.

3.3 Falhas em sistemas de logs

Logs são responsáveis por prover detalhes sobre o que está acontecendo na rede, quais sistemas estão sendo atacados e os que foram de fato invadidos[6]. O log será responsável por identificar o que foi invadido e como foi feita esta invasão.

4. Considerações Finais

Devido ao grande crescimento da utilização de computadores, da necessidade de armazenar arquivos, traçar metas e estratégias para fazer com que suas informações não sofram nenhum dano, como roubo, modificação ou perda e sejam armazenadas de formas seguras tanto fisicamente quanto abstratamente é fundamental atualmente, porque a informação hoje em dia nunca foi tão valorizada. Ter uma política sólida e bem feita, manter os usuários sempre treinados e atualizados com as ameaças que a cada dia surgem é crucial para a segurança e o desenvolvimento da corporativa. Tomando as devidas providências a corporativa estará segura, mas salientando que não existem sistemas absolutamente seguros, sempre existem falhas.

Neste trabalho foram abordados temas como política de segurança, onde se determina as metas, o que será protegido e o que ensinar aos usuários, os ataques e ameaças mais conhecidos, métodos de proteção, segurança física, os pontos falhos, problemas com senhas fracas, *backups* falhos que não são testados diariamente e problemas no sistema de logs, visando auxiliar não só as corporativas como também usuários domésticos, para que ambos não passem por situações incomodas como perder dados importantes e sigilosos.

Conclui-se que o problema principal em uma corporativa para quanto à segurança da informação é o usuário e a irresponsabilidade de profissionais da área de informática. O usuário precisa ser muito bem treinado antes de ter contato a tais informações, não passar suas senhas para ninguém e não abrir e-mails suspeitos. Já os profissionais, necessitam fazer uma reciclagem, para por em prática o que eles já sabem, para não prejudicar a corporativa. Porém, não adianta treinar bem o usuário se nas ferramentas de proteção existir brechas, como portas abertas e antivírus desatualizado e má configuração de *firewall*, como também não adianta ter ferramentas de proteção bem configuradas, se o usuário não tem treinamento.

Este artigo visa contribuir para que as empresas estejam sempre mais atentas aos riscos que elas correm para que não tenham problemas de insegurança. Saliento o quanto é necessário aos usuários possuírem treinamento adequado para não trazer danos para as corporativas, assim como, os profissionais devem estar preparados para enfrentar situações de insegurança na corporativa.

5. Bibliografia

[1] TANENBAUM, Andrew S. Redes de Computadores.4 ed. Rio de Janeiro: CAMPUS, 2003

[2]TAVARES, Emerson Rodrigo Alves. **Segurança em Redes.** UFMG, 2002.

[3]MAGALHÃES, Wanderson Fernandes. **Segurança da Informação em Redes Corporativas.** Barbacena: UNIPAC/FACICS, 2004.

[4]SOARES, Luiz Fernando Gomes. LEMOS, Guido. COLCHER, Sérgio. **Redes de computadores.** 2 ed. Rio de Janeiro: CAMPUS, 1995.

[5]DE SOUZA, Leonardo Henrique Lima. **Segurança Física de Redes de Computadores.** Rio de Janeiro: Universidade Estácio de Sá, 2004.

[6]COULOURIS, George. DOLLIMORE, Jean. KINDBERG, Tim. **Sistemas Distribuídos Conceitos e Projeto.** 4 ed. Rio Grande do Sul: BOOKMAN, 2007.