UNIVERSIDADE LUTERANA DO BRASIL

CENTRO DE CIÊNCIAS NATURAIS E EXATAS

CURSO SUPERIOR DE TECNOLOGIA EM INFORMÁTICA

UM GUIA PARA IMPLANTAÇÃO DE SEGURANÇA BÁSICA EM SISTEMAS

ADRIANA APARECIDA SETTE

ORIENTADOR: FRANCISCO ASSIS M. DO NASCIMENTO

CANOAS, NOVEMBRO DE 2001

SUMÁRIO

LISTA DE FIGURAS

RESUMO

Este trabalho visa apresentar um estudo de alguns dos principais problemas que podem ocorrer por falta de segurança básica nas empresas e propor medidas de segurança para a prevenção destes problemas.

Além disso, este trabalho demonstrará exemplos dos problemas, vivenciados na prática pela AUTORA, assim como, fornecerá os detalhes técnicos relacionados com cada medida de segurança sugerida, visando sempre uma linguagem simples, com o objetivo de através do fácil entendimento, reduzir a probabilidade de problemas por falta de segurança básica nas empresas.

Para provar a viabilidade e a eficácia das medidas sugeridas, será demonstrado como estas medidas podem ser implantadas, através do relato da implantação e da apresentação dos resultados obtidos em uma empresa de grande porte.

ABSTRACT

This work aims to show a study of some of the main problems that can occur in the companies that do not have a basic security and suggest ways of security to prevent these problems.

Moreover, this work will show examples of the problems, experienced by the AUTHOR, as well as, it will supply the technician details related with each way of security suggested, aiming always a simple language, objectifying, through the easy understanding, to reduce the probability of problems occurs in the companies for lack of basic security.

To prove the viability and the effectiveness of the suggested ways of security, it will be demonstrated how these ways of security can be implanted, through the story of the implantation and the presentation of the results gotten in a big company.

INTRODUÇÃO

Atualmente é fato que somos dependentes do computador e o uso desta tecnologia é hoje, irreversível e cresce a cada dia, fazendo com que as empresas que não aderiram ainda a tudo isso, tornem-se obsoletas, arcaicas e tenham prejuízos [FON 00].

A rapidez com que surgem novas facilidades e avanços tecnológicos é assustadora, uma empresa termina de atualizar seus softwares para uma nova versão e em seguida são lançados softwares ainda mais avançados, estes avanços tecnológicos proporcionam grandes facilidades como, por exemplo, agilidade, confiabilidade, rapidez, controle de informações, entre outras.

Mas tudo isso também traz problemas, pois a dependência desta tecnologia faz com que um defeito num computador ou um problema em um software, coloque em risco anos de trabalhos e estudos.

Além disso, no momento em que os sistemas passaram a compartilhar os dados e conectar as redes, aumentaram os problemas por falta de segurança, pois quando muitos acessam as informações são necessários cuidados para que não haja acessos indevidos e mau uso do sistema.

Muitos acessos e o controle de servidores, que antigamente eram mantidos por uma pessoa, com um conhecimento básico ou nenhum de segurança, agora é compartilhado entre várias pessoas, que podem estar no mesmo prédio ou em continentes diferentes, tornando mais difícil o controle de quem acessa as informações da empresa.

Claro que antigamente também existiam problemas de segurança, mas eram em proporções muito menores que hoje e mais simples de serem resolvidos. Hoje em dia existem pessoas comuns controlando sistemas importantes da empresa, muitas delas não acompanharam a evolução dos problemas de segurança e não possuem o conhecimento necessário para se prevenir contra novos problemas que aparecem a cada dia [XIM 00].

Segundo estatísticas, sobre os incidentes de segurança registrados neste ano, até setembro, divulgadas recentemente pelo Computer Emergency Response Team (CERT/CC), centro de pesquisas em segurança na Internet da Universidade de Carnegie Mellon, o número de incidentes até setembro de 2001 já superou em mais de 50% o total de registros do ano de 2000 [CER 01].

Devido ao constante crescimento de problemas por falta de segurança, as empresas que possuem sistemas de informação devem ter como prioridade nas suas estratégias a preocupação com a prevenção destes problemas, mas precisam estar preparadas, pois existem muitos fornecedores oferecendo seus produtos e serviços de segurança como capazes de resolver todos os problemas de segurança da empresa, convencendo pessoas inexperientes que, contratando os serviços destas empresas ou instalando seus produtos, estarão totalmente seguras.

Mas a realidade é que nenhum sistema ou serviço é 100% seguro, o que existe são várias medidas de segurança que, implantadas em conjunto com algum produto, vão diminuir os riscos de problemas de segurança.

Fontes, em um dos seus artigos, exemplifica isso dizendo que segurança da informação não é apenas uma atitude ou um produto ou uma pessoa, são muitas atitudes [FON 99], que implementadas vão proteger a organização, e tornar a segurança da informação efetiva. Não adianta gastar um valor exorbitante para colocar porta com senha de acesso nas salas onde estão os servidores da empresa, se não existe um procedimento de controle de acessos e a senha é conhecida por todos e não é trocada regularmente. Não adianta ter um perfeito software de backup e um cofre em outra planta da empresa, para onde as fitas levadas, se diariamente este backup não for conferido se foi realizado corretamente.

É importante salientar que cada empresa tem uma realidade e, devido a isso, uma solução de segurança, proposta para uma empresa, pode não ser a solução ideal para outra empresa, que trate de negócios diferentes.

O estudo, a que se propõe este trabalho, está baseado em uma pesquisa teórica, conforme referências Bibliográficas, revistas, jornais e demais mídias atuais, assim como, pelo acompanhamento na prática, pela AUTORA, que vivenciou estes problemas em mais de uma empresa e pode mensurar os efeitos e as conseqüências destes problemas na realidade, como também, conhecer as diferenças de quando se tem medidas de segurança implantadas e mantidas.

Portanto, este trabalho citará problemas gerais que qualquer tipo de empresa está exposta, as medidas de segurança para prevenção destes problemas, propostas neste trabalho, podem ser usadas por qualquer empresa, mas serão soluções básicas que deverão ser trabalhadas em conjunto para se tornarem efetivas.

Mas, para que a empresa fique tranqüila, no que diz respeito a segurança, a implantação destas medidas é apenas o começo, sempre será necessário o comprometimento dos funcionários, o apoio da alta direção da empresa e o acompanhamento de novas tecnologias e novos riscos, ou seja, é um trabalho que exige continuidade.

1 ASPECTOS IMPORTANTES NA ÁREA DE SEGURANÇA DE SISTEMAS

1.1 Autenticação

Todo acesso a um determinado local, arquivo, computador ou sistema ao ser autenticado, significa que este acesso é verdadeiro, ou seja, que a pessoa ou sistema que está solicitando o acesso é mesmo quem afirma ser.

Esta autenticação é feita através de: senha criptografada, onde a senha é codificada, dificultando assim, que alguém possa decifrá-la; cartões inteligentes, que são semelhantes a cartões de créditos, porém são mais avançados, pois podem armazenar dados; assinatura digital, que é um método baseado em criptografia com chave pública para confirmar uma identidade; senhas ocasionais, que só podem ser utilizadas uma vez; biométrica, que utiliza características físicas dos usuários, como digitais e impressões da retina, para serem autenticados, entre outros.

Existe também, a autenticação de dois fatores e a autenticação rígida, na primeira, dois tipos de autenticação são necessários para provar a identidade de alguém, como uma senha e um cartão inteligente, já na autenticação rígida a execução se baseia em critérios muito específicos, como senhas ocasionais mecanismos de desafio/resposta e a autenticação criptográfica.

Após a autenticação, o próximo processo importante é a autorização, onde é determinado no que a pessoa autenticada terá acesso, que tarefas poderá executar e com que privilégios.

Para verificação das informações sobre eventos a respeito de quem acessou, em que horário, que arquivos ou sistemas foram acessados, entre outros, muitos sistemas possuem um LOG de registros com estas informações, mas este recurso, geralmente, precisa estar ativado para gerar informações.

1.2 Criptografia

A palavra Criptografia é formada por duas palavras, Cripto e Grafia. Cripto significa ocultar, esconder e Grafia é a escrita, ou seja, é a arte da escrita secreta, é a prática de codificar dados que são decodificados depois, pela decriptografia. A Criptografia é muito antiga, um exemplo de criptografia é a linguagem do “P”, utilizada como brincadeira de criança, quem não sabia decifrar esta linguagem, não entendia o assunto que estava sendo tratado [PAN 00].

Existem as criptografias fracas, que são mais fáceis de decifrar e as criptografias fortes, que são consideradas difíceis de serem decifradas, ou até impossíveis, até o momento que alguém consiga decifrá-las. Para uma criptografia ser considerada forte, ela tem que mudar pelo menos 50% do resultado final ao ser alterado um caractere no texto original ou o mínimo possível na chave de criptografia.

Para encriptar é utilizado um algoritmo para transforma o texto simples em texto cifrado, como no exemplo citado acima, da linguagem do “P”, suponhamos que a palavra a ser encriptada seja “criança”, aplicando-se o algoritmo que é incluir a letra P na frente de todas as sílabas, o texto encriptado será “Pcri-Pan-Pça”, para decriptá-lo, deve-se aplicar o mesmo algoritmo de maneira inversa.

Os algoritmos utilizados podem ser restritos ou com a utilização de chaves. Algoritmo restrito é baseado em manter-se em segredo, mas a sua falha está em que, onde for utilizado por muitas pessoas, seu código poderá ser descoberto. Mas existem os algoritmos que utilizam chaves para encriptar e decriptar um texto, que podem Simétrico ou Assimétrico.

A criptografia Simétrica, também chamada de algoritmo simétrico ou criptografia de chave simples ou, ainda, de criptografia convencional, é uma criptografia tão forte que seus algoritmos são de acesso público.

Para criptografar, coloca-se o texto a ser criptografado junto com a chave em um polinômio e o resultado é o texto encriptado, conforme mostra a figura 1.2.1.

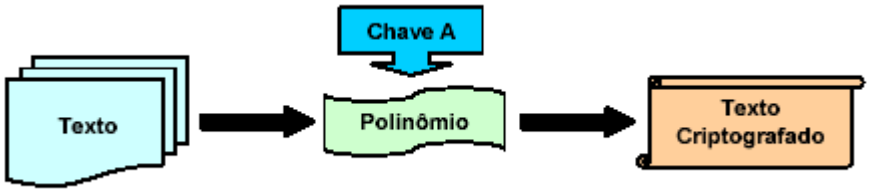

Figura 1.2.1: Criptografia Simétrica – Criptografar [PAN 00]

Para o processo inverso, deve ser aplicado o polinômio com o texto criptografado e mais a chave aplicada na criptografia e o resultado é o texto original, conforme figura 1.2.2.

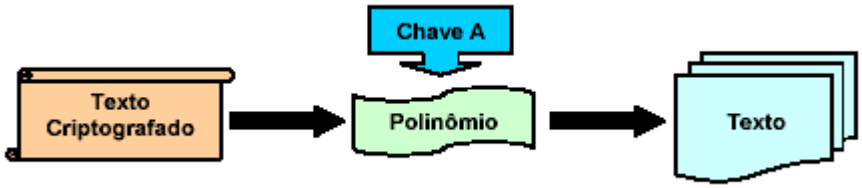

Figura 1.2.2: Criptografia Simétrica – Decriptografar [PAN 00]

Esta criptografia tem como vantagem a rapidez e a utilização de chaves pequenas. A grande desvantagem é que a chave que encripta é a mesma que decripta, ou seja, para o destinatário poder ler uma mensagem com esta criptografia, é necessário enviar junto, a chave que decripta, como é a mesma que encripta, o destinatário poderá decriptar diversos arquivos da máquina de origem.

Embora com esta desvantagem, os polinômios simétricos são muito utilizados, principalmente pelas suas vantagens. Alguns exemplos são: DES, IDEA, CAST, RC2, 3DES, entre outros.

Para resolver a falha do algoritmo assimétrico, a maneira criada foi um mesmo algoritmo, após a entrada de alguns dados, gerar duas chaves, uma para encriptar e a outra para decriptar, demostrado na figura 1.2.3.

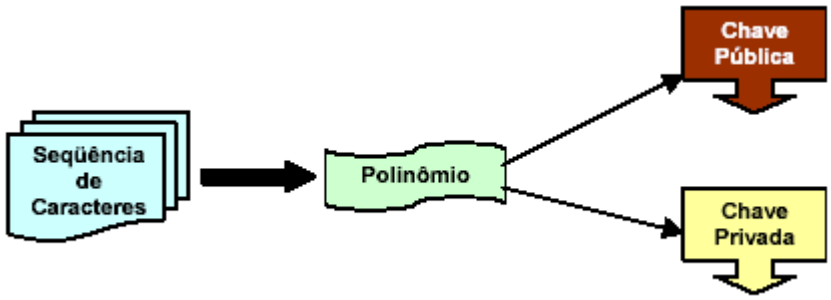

Figura 1.2.3: Criação do par de chaves [PAN 00]

Este algoritmo é utilizado na criptografia Assimétrica, que geralmente é a mais eficiente e é usada para intercâmbio de chaves e assinaturas digitais.

Nesta criptografia, utiliza-se uma chave privada, que geralmente é mantida em segredo pelo seu proprietário e uma chave pública, na maioria das vezes é divulgada para todos, ou seja, a chave que encripta é diferente da que decripta.

Como mostra a figura 1.2.4, para encriptar, pega-se a chave pública, junto com o polinômio ou algoritmo e aplica-se no texto simples, para resultar no texto criptografado.

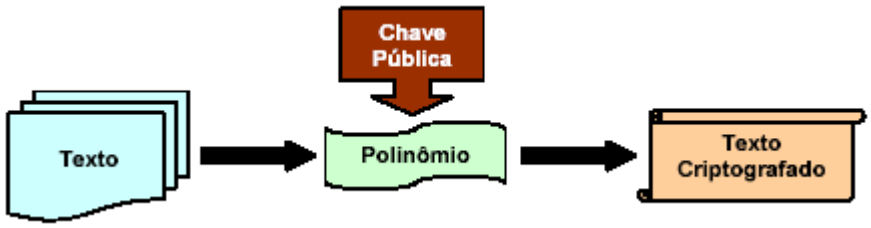

Figura 1.2.4: Criptografia Assimétrica – Criptografar [PAN 00]

Para decriptar este texto, deve ser utilizado a chave privada, aplicando-se esta chave, junto com o mesmo polinômio (ou algoritmo) da criptografia, no texto criptografado e o resultado é o texto original, como mostra a figura 1.2.5.

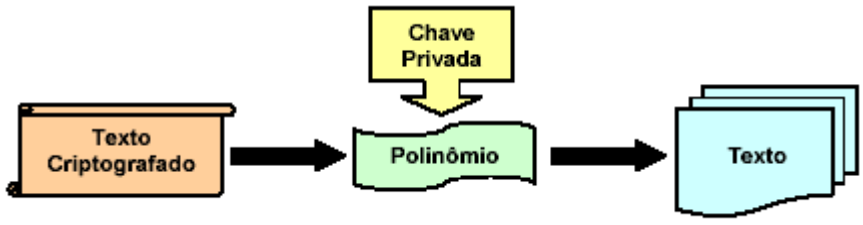

Figura 1.2.5: Criptografia Assimétrica – Decriptografar [PAN 00]

A grande vantagem deste algoritmo é ter chaves diferentes para encriptar e decriptar, o grande problema é que este algoritmo é lento, demora bem mais tempo que o algoritmo simétrico para encriptar um texto e as chaves são grandes. Alguns exemplos de algoritmos assimétricos são Diffie Hellmann, RSA, ElGamal, DSS.

Existe uma solução de criptografia que utiliza as vantagens dos dois algoritmos citados acima, esta solução é chamada de Criptosistemas Híbridos.

Dentro de um sistema de criptografia com chave pública, existe uma autoridade de certificação, conhecida apenas por CA, que é um recurso que, após determinar os usuários e suas funções válidos para este sistema, emite chaves e certificados correspondentes. Então, certificado é lista destes usuários. Sempre que um usuário ou uma função for revogado desta lista, ou seja, passar de válido para inválido, este usuário ou função será incluído no CRL, que é uma lista de revogação de certificados.

1.3 Técnicas de Invasão

Invasão é a entrada em um site, servidor, computador ou serviço por alguém não autorizado. Mas, antes da invasão propriamente dita, o invasor poderá fazer um teste de invasão, que é uma tentativa de invasão em partes, onde o objetivo é avaliar a segurança de uma rede e identificar seus pontos vulneráveis.

Mas não existe invasão sem um invasor, que pode ser conhecido, na maioria das vezes, como hacker ou cracker. Ambos usam seus conhecimentos para se dedicarem a testar os limites de um sistema, ou para estudo e busca de conhecimento ou por curiosidade, ou para encontrar formas de quebrar sua segurança ou ainda, por simples prazer.

Mas também pode ser por mérito, para promoção pessoal, pois suas descobertas e ataques são divulgados na mídia e eles se tornam conhecidos no seu universo, a diferença é que o cracker utiliza as suas descobertas para prejudicar financeiramente alguém, em benefício próprio, ou seja, são os que utilizam seus conhecimentos para o mau [SEC 03].

Existem muitas ferramentas para facilitar uma invasão e a cada dia aparecem novidades a respeito. Abaixo serão descritas algumas das mais conhecidas.

1.3.1 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 o seu endereço de origem. É uma técnica de ataque contra a autenticidade, onde um usuário externo se faz passar por um usuário ou computador interno [SPO 01].

1.3.2 Sniffers

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 de 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.

1.3.3 Ataque do tipo DoS

É um ataque de recusa de serviço, estes ataques são capazes de tirar um site do ar, indisponibilizando seus serviços. É baseado na sobrecarga de capacidade ou em uma falha não esperada.

Um dos motivos para existirem este tipo de falha nos sistemas é um erro básico de programadores, na hora de testar um sistema, muitas vezes, eles não testam o que acontece se o sistema for forçado a dar erro, se receber muitos pacotes em pouco tempo ou se receber pacotes com erro, normalmente é testado se o sistema faz o que deveria fazer e alguns erros básicos. O invasor parte deste princípio e fica fazendo diversos tipos de testes de falhas, até acontecer um erro e o sistema parar.

Este tipo de ataque não causa perda ou roubo de informações, mas é um ataque preocupante, pois os serviços do sistema atacado ficarão indisponíveis por

um tempo indeterminado, dependendo da equipe existente na empresa para disponibilizá-lo novamente e dependendo do negócio da empresa, este tempo de indisponibilidade pode trazer muitos prejuízos [MSK 99].

Em maio deste ano, foi divulgada pela Modulo [SEC 03], a descoberta de novos tipos de Ataques Dos. Esta nova geração inclui o “pulsing zombies”, que envia curtas emissões de tráfego a um alvo determinado e não contínuo como no ataque já conhecido, que podem ser rastreados. Esta nova maneira de ataque dificulta ainda mais a detecção.

Além disso, técnicos da empresa Asta Networks, responsáveis por esta identificação, descobriram que, neste novo tipo de ataque em vez de paralisar totalmente o servidor, ele apenas restringe seus serviços. Os servidores atacados, desta maneira, não ficam sobrecarregados, mas sim, confusos com o grande número de atividades de rede.

E, de acordo com um estudo da Universidade da Califórnia, crackers tentam realizar em torno de 4 mil ataques do tipo DoS por semana. O alvo mais comum são grandes empresas [SEC 03].

1.3.4 Ataque do tipo DDoS

São ataques semelhantes ao DoS, tendo como origem diversos e até milhares pontos disparando ataques DoS para um ou mais sites determinados. 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.

1.3.5 DNS Spoofing

O objetivo principal do DNS Spoofing é destruir o servidor de nomes e com isto permitir que máquinas não confiáveis, que podem ser as do invasor, sejam consideradas confiáveis, pois se passarão pelas confiáveis. Para realizar este ataque, o invasor precisa ter o controle sobre a máquina servidora de DNS, Domain Name Server, onde constam todos os nomes das máquinas confiáveis e os endereços destas máquinas, que são os números IP. Além disso, o invasor precisará saber o nome de uma destas máquinas confiáveis.

Com posse destes dados, o invasor altera registro do DNS que mapeia o endereço IP da máquina confiável escolhida modificando para que contenha o endereço da máquina do invasor. A partir desta alteração, o invasor terá livre acesso em serviços que necessitam a autenticação deste servidor de nomes [SPO 01].

A maioria dos novos sistemas possuem métodos contra o DNS Spoofing, utilizando uma técnica chamada cross-check. Nesta técnica, o nome retornado pela consulta é testado novamente pelo DNS. Se o endereço utilizado para a conexão é diferente do retornado pelo cross-ckeck, a conexão é bloqueada e é gerado um alerta. Esta técnica pode ser implementada no servidor de DNS ou nos servidores dos serviços com autenticação baseada no DNS.

Mas, existem variantes do DNS Spoofing, onde o invasor tenta enganar o croos-check, esgotando o servidor de DNS com pedidos.

1.3.6 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. 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.

1.3.7 Vírus

O vírus de computador é outro exemplo de programa de computador, utilizado maliciosamente ou não, que se reproduz embutindo-se em outros

programas. Quando estes programas são executados, o vírus é ativado e pode se espalhar ainda mais, geralmente danificando sistemas e arquivos do computador onde ele se encontra, um exemplo deste tipo de programa é o Worm.

Outro exemplo de vírus muito conhecido é o Trojan, que insere um trecho de código em um programa aparentemente inofensivo e assim, coloca um hospedeiro no site invadido, onde o invasor fica com o controle remoto do sistema.

Segundo pesquisa realizada por uma empresa britânica de antivírus, o número de ataques de vírus deve triplicar até o final do ano. Nesta pesquisa também pode ser concluído que as ferramentas para proteção efetiva contra os vírus não terão o mesmo crescimento [SEC 01].

1.3.8 Demais considerações sobre Técnicas de Invasão

Por fim, o invasor pode utilizar-se da evasão, que é a arte de não deixar pistas de quem invadiu e como isto aconteceu, e quando isto é feito com êxito, dificulta ainda mais a descoberta desta vulnerabilidade e, assim, da correção da mesma, para se proteger de novos ataques.

1.4 Ferramentas de segurança

Existem no mercado, diversos tipos de ferramentas, para proteger sistemas ou detectar invasões. Em seguida serão descritas algumas mais conhecidas.

1.4.1 Firewalls

Quando o assunto é segurança, uma das primeiras ferramentas mencionadas é o Firewall, no sentido amplo, ele nega o acesso de usuários não autorizados a um determinado host ou arquivo, em sentido restrito, ele examina cada pacote e determina a origem, se está em uma lista aprovada ele permite o acesso, senão, não libera. Já numa definição mais usual ele é uma barreira de proteção entre duas redes, geralmente, ele fica entre a rede local e a Internet [PAU 00].

Segundo Anchises, é chamado de firewall o equipamento que garante o controle da conexão entre duas ou mais redes, ou seja, é um equipamento que roda uma aplicação específica de controle de acesso e que é responsável por interligar, de forma segura, duas ou mais redes, garantindo o controle, a verificação e o log (auditoria) dos pacotes que passam entre elas. Seu nome foi originado das paredes corta-fogo, existentes para impedir a passagem do fogo em prédios.

Firewall filtra os acessos feitos da empresa para a internet e da internet para a empresa. Num dos artigos de Carissimi ele explica que o Firewall [CAR 00], apesar de ser uma ferramenta de extrema importância para a proteção da empresa de acessos indevidos externos, a utilização dele isoladamente não garante segurança.

A solução, segundo ele, é implantar duas medidas de segurança, Política e Controle. A empresa deve ter uma Política de Segurança que descreva o papel dos recursos de TI dentro da empresa, e elaborar mecanismos para controlar estas políticas, estas medidas estão descritas no capítulo 4.

Isto mostra que o Firewall protege a rede interna de ataques externos, mas não de ataques internos. Além disso, o Firewall quanto instalado corretamente é uma barreira contra ataques, mas caso o invasor consiga quebrar a segurança do Firewall ou este estiver mal configurado, o invasor terá acesso ao sistema.

1.4.2 Sistemas de Detecção de Intrusão

São sistemas inteligentes, capazes de detectar tentativas de invasões em tempo real. Estes sistemas podem apenas alertar sobre a invasão, como, também, aplicar ações necessárias contra o ataque. Eles podem ser Sistemas baseados em regras ou adaptáveis, no primeiro as regras de tipos de invasões e a ação a ser executada são previamente cadastradas. O problema é que a cada dia surgem novos tipos de ataques e estas regras precisam estar sempre atualizadas para o sistema ser eficaz. No segundo tipo, são empregadas técnicas mais avançadas, inclusive de inteligência artificial, para detectarem novos ataques, sempre que surgirem.

Além disso, o sistema de detecção de intrusão pode ser classificado como NIDS (sistema de detecção de intrusão de redes) e HIDS (sistema de detecção de intrusão de hosts).

1.4.3 Logs

Logs são registros gerados pelos sistemas ou aplicações, sobre informações de eventos ocorridos. É considerado uma medida básica de segurança, mas muitas vezes não é utilizado pelos administradores, ou por que está desativado, pois dependendo do sistema e do hardware, a geração do Log pode se tornar lenta, ou por que esquecem ou não querem analisá-lo, já que os logs geralmente são relatórios enormes. Mas é uma ferramenta útil para auditorias de acessos, verificação do que está sendo utilizado, possível falha nos sistemas, entre outros.

1.4.4 Antivírus

Software que verifica a existência de vírus em uma máquina, pasta, arquivo e ao encontrá-lo, executa a limpeza. A maneira como ele fará isso pode ser totalmente configurada pelo usuário. O padrão é o antivírus analisar e quando encontrar algum vírus tentar eliminar apenas o vírus, caso não consiga, se o usuário autorizar, ele removerá o arquivo também. Uma vez instalado o antivírus em um micro, ele pode

ser configurado, dependendo da sua característica, para ficar ativo e analisar tudo que for aberto no micro, caso apareça algum vírus, ele avisa imediatamente.

Mas como diariamente surgem novos tipos de vírus, diariamente também, a lista de vírus dos antivírus é atualizada, neste caso, é importante o usuário ficar atento a atualizar o seu antivírus sempre que possível.

1.4.5 Backup

Uma das ferramentas existentes para segurança dos dados são os softwares de backup e restore, que servem para fazer cópias de segurança das informações e sistemas de uma empresa e recuperar as informações quando necessário. Todos os dados e sistemas de uma empresa devem possuir cópias de segurança íntegras, atuais e armazenadas em local seguro.

Em geral, o backup é feito em fita, disquete ou outra mídia portátil que pode ser armazenado para futura utilização, como no caso de algum desastre ou perda de informações. As informações podem ser perdidas por causa de acidentes, desastres, ataques, erros de sistemas ou hardwares ou falha humana, entre outros motivos. Com as informações atualizadas copiadas através de backups para alguma mídia, quando houver uma perda de dados, basta restaurar estas informações.

1.5 Legislação no Brasil

O Código Penal Brasileiro foi criado em 1940 e é aplicado atualmente. Na época em que foi criado não era possível prever a explosão tecnológica que está acontecendo nos últimos anos e muito menos os crimes digitais que ela originou.

Com tudo isso, segundo Olavo Gomes [GOM 01] a alternativa encontrada foi a utilização de um artigo da Lei de Telemática e embora seja grande o esforço para punir os criminosos digitais, geralmente, ou o processo é arquivo ou o réu é absolvido por falta de enquadramento jurídico.

Mas, nos últimos anos é grande o esforço para acabar com a impunidade dos crimes digitais. Para isso estudiosos e Autoridades Governamentais estão elaborando diversos projetos de Lei como os seguintes:

- Projeto de Lei 234/96 – Define crime contra a inviolabilidade de comunicações de dados de computador (Infojur – UFSC).
- Projeto de Lei 3258/97 Dep. Osmânio Pereira – Define crimes cometidos através de redes de informação.
- Projeto de Lei 84/99 – Dispõe sobre crimes cometidos na área de informática, suas penalidades e outras providências.

- Projeto de Lei 713/95 – Dispõe sobre as irregularidades e crimes que podem ocorrer no meio eletrônico das redes de computadores e da Internet e as suas possibilidades.

Demais informações podem ser encontradas no site jusnavegandi.com.br.

Além disso, existe a norma oficial britânica sobre o gerenciamento da segurança da informação, a ISO/IEC 17799:2000 e baseada nela, a Associação Brasileira de Normas Técnicas (ABNT) está propondo um projeto de elaboração de uma norma brasileira sobre segurança da informação.

Os principais pontos desta norma são: política de segurança da informação, conformidade, segurança organizacional, classificação e controle dos ativos de informação, segurança física e do ambiente, gerenciamento das operações e comunicações, controle de acesso, desenvolvimento, manutenção de sistemas e gestão da continuidade do negócio [SEC 03]. Quando aprovado este projeto receberá a numeração NBR ISO/IEC 17799:2001.

1.6 Demais aspectos

Outros aspectos importantes na área de segurança da informação são sobre as falhas dos sistemas, os nomes Bug, Falhas, Vulnerabilidade, são familiares, mas

como serão citados posteriormente neste trabalho, se torna importante explicar um pouco do significado destes termos.

Um Bug é uma falha ou fraqueza de programação em um sistema, que o faz executar incorretamente, resultando em mensagens de erros ou simplesmente parando completamente o sistema. Já a vulnerabilidade, refere-se a qualquer fraqueza, ou bug, em quaisquer sistemas, seja de hardware ou software, que permite que invasores ganhem acessos não autorizados ou neguem algum serviço.

2 PRINCIPAIS PROBLEMAS

2.1 Acessos indevidos, internos e externos

Este é um dos principais problemas citado por Fontes [FON 00] e em diversas revistas e livros sobre o assunto, ele prejudica tanto a imagem da empresa, como pode trazer muitos prejuízos financeiros, pois os acessos à informações sigilosas, podem ser usados contra a empresa ou serem divulgados à imprensa ou a concorrência e, dependendo do negócio, qualquer uma destas ações é prejudicial.

Estes acessos podem ser internos ou externos e podem ocorrer por que o sistema de segurança existente possui falhas, deixando a segurança aberta, ou por que não existe segurança. Algumas das causas são os acessos desatualizados, como os acessos de ex-funcionários não removidos, usuários com acessos desnecessários ou que não utilizam mais.

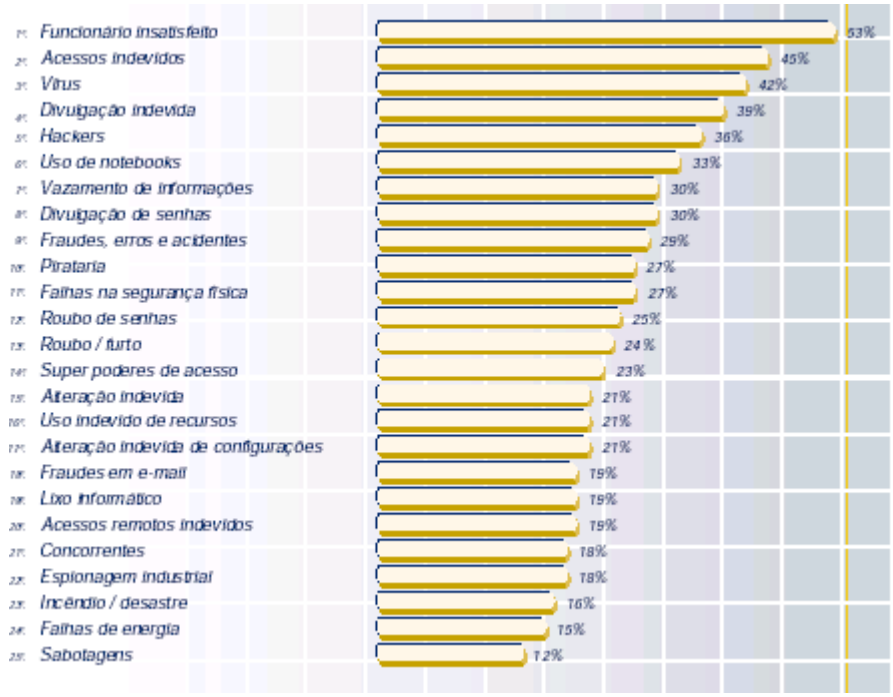

Figura 2.1: Principais Ameaças [PNS 01]

Os ataques internos são hoje, um dos grandes problemas nas empresas, segundo pesquisa feita pela MIS Training Institute, baseada em um estudo específico do governo e das empresas dos EUA [FAV 00], o hacker está dentro das empresas, a pesquisa revela que quanto a honestidade dos funcionários 40% são inerentemente honestos, 30% são capazes de cometer desonestidade, caso sejam dadas condições favoráveis para isso e 30% estão procurando um meio de obter acesso e explorar “facilidades”.

Alguns dos ataques são involuntários, simplesmente por que o usuário não tem o conhecimento correto dos recursos que está utilizando e prejudicando algum serviço por causa disso, mas outros ataques são com intenções maldosas, tentam acessar informações sigilosas para usar contra a empresa ou simplesmente tentam

indisponibilizar algum serviço para prejudicar a empresa, estes casos na maioria das vezes são de funcionários insatisfeitos. Conforme figura 2.1.

Geralmente quando entra um novo funcionário é criado um acesso nos sistemas com uma senha padrão, neste momento ele pode estar recebendo acessos a sistemas que não são necessários ou acessos a sistemas que não está apto a utilizar ainda, ou ele está trocando de setor e apenas solicitou acesso aos sistemas do novo setor sem avisar que podem ser removido os acessos anteriores, ou ainda, ele está sendo demitido, mas não foi avisado ao setor responsável e o acesso dele ainda existe.

Pode-se citar também o exemplo de pessoas com super poderes, que muitas vezes, por falta de tempo, passam o seu acesso e a sua senha para um estagiário ou outro funcionário que não tem os mesmos acessos, para que desenvolvam o mesmo trabalho, com a intenção de ganhar tempo ou serem mais produtivos. Ou até mesmo, esta pessoa com superpoderes pode cometer erros, na maioria das vezes por falta de conhecimento.

Existe um outro tipo de usuário que tenta descobrir o que ele pode acessar e começa a entrar em tudo que ele tem acesso, se neste momento ele descobrir algum acesso que não devia, ele dificilmente avisará ao setor responsável, ele continuará pesquisando. Numa empresa onde a AUTORA trabalhou, um usuário com esta atitude descobriu que tinha acesso às máquinas do setor de custos e que

nestas máquinas havia muitos arquivos interessantes, como salários pagos, gastos com eventos, gastos de gerentes, entre outras informações muito importantes para ficarem abertas para o conhecimento de qualquer pessoa, ou até mesmo, para a alteração ou remoção de arquivos importantes.

Outro exemplo é quando numa empresa com uma equipe de suporte à informática especializada, todos com acesso a todos os arquivos da rede, pois precisam disso para dar suporte, alguns até com super poderes e, quando entra um funcionário novo, que ainda não foi treinado, acabam dando a ele os mesmos acessos que o restante da equipe, ele pode remover algo importante, tirar o acesso de algum usuários ou dar um acesso indevido para outro, apenas por falta de orientação.

Na 7ª pesquisa sobre segurança da informação realizada pela Modulo em julho de 2001 [PNS 01], aproximadamente 53% das empresas apontam os funcionários insatisfeitos como a maior ameaça à segurança da informação, ou seja, mais uma vez se, uma mostra de que um dos maiores problemas vem de dentro da empresa. Conforme mostra a figura 2.1.

2.2 Vulnerabilidade de softwares

Vulnerabilidades de software é um dos problemas mais perigosos, não só pelos riscos que causa, mas principalmente por ser ignorado por muitos técnicos de

informática. Segundo estatísticas do CERT [CER 01], em 1999 o número de vulnerabilidades reportadas foi de 417, quase o dobro do ano anterior, em 2000 este número subiu para 1090, sendo que em 2001, somente até o terceiro trimestre foram reportadas 1820 vulnerabilidades.

Estas vulnerabilidades são divulgadas na Internet, grupos de segurança ou em revistas especializadas. Assim como são divulgadas as falhas de sistemas, também são divulgadas as correções para estas falhas que devem ser aplicadas no sistema vulnerável, o problema é que muitos usuários não ficam sabendo e, assim, não aplicam a correção para resolver a falha, deixando seu sistema trabalhando de forma vulnerável. Só que os intrusos, conhecem bem estas falhas e por saberem que muitos usuários não aplicam a correção, exploram estas vulnerabilidades para invadir um sistema.

Segundo o autor de Segurança Máxima [XIM 00], existem dois tipos de falhas de sistemas, o primeiro tipo, denominado por ele como falhas primárias, trata de um defeito colocado dentro da estrutura de segurança do sistema operacional. É uma falha, que sozinha não teria tantos problemas, mas por estar ligada internamente em um programa relacionado com segurança pode trazer sérios problemas se for usada por um invasor. As falhas secundárias são mais comuns, são as falhas que aparecem em muitos aplicativos, não relacionados com segurança, mas abre uma brecha de segurança em outra área do sistema. O maior motivo de acontecerem

tantas falhas deste tipo é por que geralmente os programadores estão dando importância para a funcionalidade do sistema e não para a segurança.

Um motivo que torna este problema ainda mais ameaçador é que a maioria destas vulnerabilidades só aparece quando o sistema já está sendo usado por muitos usuários, muitas vezes são descobertas pelo próprio usuário após ter sido alvo de algum problema de segurança, ou são descobertas por algum hacker que após diversas tentativas de quebrar a segurança do novo sistema ou da nova versão, obteve êxito e divulgou.

Em qualquer dos casos, pode acontecer do fornecedor já possuir estudos sobre a falha, geralmente a correção vem rápido, mas para o fornecedor esta divulgação sempre é negativa e ele acaba não divulgando eficientemente. Pois para ele não é interessante alguém descobrir falhas no seu sistema, será uma repercussão negativa para a sua empresa.

A correção pode demorar ainda mais se a falha estiver afetando outros sistemas ou se o sistema está em produção numa empresa. Pode acontecer também de não existir suporte para o software quando o fornecedor comprou o sistema de outro fabricante, ou até mesmo o fabricante estar estudando a correção sem uma previsão de quando será liberada a correção e muitos outros exemplos.

Nestes casos os usuários sem conhecimento necessário sobre os sistemas que utilizam e se não estiverem atualizados sobre o que está acontecendo ao seu redor, serão mais uma vítima de um ataque ou outro problema por falta de segurança, o que o faz estar ligado ao próximo problema que é a falta de conhecimento.

2.3 Usuários sem conhecimentos necessários

Este problema foi citado no livro segurança máxima, onde um hacker explica que existem 3 grandes problemas pela falta de segurança nas empresas e dois destes problemas estão ligados a falta de conhecimento [XIM 00].

Antigamente as informações e conhecimentos sobre segurança ficavam nas mãos de poucos, na época, não existia a necessidade de muita segurança, pelo menos os usuários não precisam se preocupar com isso, mas hoje é preciso um mínimo de conhecimento, pois problemas de segurança podem atacar qualquer um na empresa, a falta de conhecimento pode trazer muitos problemas de segurança.

Um exemplo disso, vivido pela AUTORA numa empresa onde a mesma trabalhou, foi o seguinte, a empresa comprou um Firewall, mas se não existir alguém na empresa para configurá-lo corretamente, então foi contratada uma empresa especializada para instalar o firewall, mas como os funcionários não

foram treinados com um mínimo de conhecimentos da ferramenta, com poucos comandos “ingênuos” eles deixaram o sistema vulnerável a ataques.

Isto acaba se tornado uma mistura entre os problemas de acessos indevidos e falta de conhecimento. Na figura 2.1, aparece os itens de alteração indevida e alteração indevida de configuração, que juntos somam 42% das principais ameaças de segurança, segunda a pesquisa [PNS 01].

2.4 Vírus de computador

É uma praga virtual, ataca desde grandes empresas, espalhando-se via rede para diversos computadores e arquivos, assim como no computador de casa, via Internet ou via disquete infectado. Já possui mais de 10 anos de existência e a cada dia surgem novos tipos, o que faz com que os softwares de vacina fiquem desatualizados precisando freqüentemente ser atualizados.

Algumas empresas que não levam a sério este problema e acabam tendo diversas máquinas ou até mesmo a rede inteira infectada por um vírus, que pode até ser inofensivo, mas para removê-lo serão necessários horas e dedicação de técnicos da área de suporte.

Uma máquina infectada pode, em segundos, acessar um arquivo da rede e infectar a rede, este arquivo da rede pode ser acessado por diversas outras

máquinas da empresa, que serão infectadas também, ou seja, até ser descoberto a primeira máquina infectada, o vírus pode ter se espalhado por quase toda a empresa, dificultado ainda mais a limpeza.

Mas se não for um vírus inofensivo, além dos problemas citados acima, podem ocorrer perda de informações, afetar a funcionalidade de algum sistema, entre outros problemas, dificultando ainda mais que a ordem seja restabelecida.

Com o E-mail vieram os vírus que chegam anexados às mensagens, muitos deles se auto-enviam para a lista de endereços da máquina infectada, como se fossem o usuário infectado, assim, a pessoa que recebe a mensagem abre o arquivo, achando tratar-se de algo confiável, já que foi enviado por um conhecido e acaba sendo infectada.

Mais uma vez, entramos no problema de falta de conhecimento, pois uma pessoa atualizada nas informações a respeito de novos vírus, sempre terá cuidado ao abrir qualquer tipo de E-mail, mesmo sendo enviado por alguém conhecido.

2.5 Ataques de Hackers, ex-funcionários ou funcionários insatisfeitos

Os ataques externos às empresas ocupam um lugar de destaque entre as principais ameaças que preocupam as empresas. Mesmo assim existem pessoas que pensam que isso está longe da realidade, que não acontecerá com elas.

Existem muitos mitos a respeito do assunto. Alguns acham que não existe nada no seu site que possa interessar os invasores, só que muitos invasores invadem apenas para colocar uma mensagem política ou uma manifestação, apenas para chamar a atenção.

Hoje, em pleno século XXI, com tanta dependência das empresas nos computadores, não é tempo de pensar que as coisas ruins só acontecem com os outros, todos precisam se prevenir, pois tempo é dinheiro e qualquer ataque externo, seja inofensivo ou não, exigirá a dedicação de tempo para que o problema seja solucionado.

Numa situação em uma empresa em que a AUTORA trabalhava, um ex-funcionário da área de informática, que tinha a senha do administrador da rede, tentou acessar o servidor de Internet da empresa, utilizou a senha que conhecia e acessou o sistema normalmente, pois a senha não havia sido trocada. O ex-funcionário, por ser uma pessoa ética, avisou o gerente de informática e foram tomadas medidas para que a senha fosse alterada freqüentemente, principalmente na saída de alguém do setor que conhecesse a senha. Mas se

este funcionário estivesse insatisfeito com a empresa, o final desta história poderia ser bem diferente.

Num ataque de funcionário insatisfeito ou um ex-funcionário, geralmente ele já possui algumas informações que facilitarão o seu acesso ilegal, mas no caso de hackers ou crackers, existem algumas técnicas utilizadas por eles para conseguirem invadir o alvo.

Primeiramente, eles irão coletar informações a respeito do alvo, através dessas informações, o invasor fará uma análise do sistema operacional da vítima e poderá escolher a estratégia ideal de ataque [NET 01].

Além de todas as ferramentas, já descritas no item 1.3, do capítulo 1, eles também exploram as vulnerabilidades conhecidas e documentadas de softwares, conforme descrições a respeito de vulnerabilidades no item 2.2 do capítulo 2.

Além disso, existe a Engenharia social, onde eles se utilizam de contatos com pessoas internas para descobrirem informações importantes da empresa ou executarem ações, que facilitem a invasão [SEC 03], o invasor obtém o que quer através da ingenuidade ou confiança da vítima. Ela pode ser feita através de telefones, salas de bate-papo, envio de mensagens e até mesmo pessoalmente. Esta técnica é considerada uma técnica avançada, se for feita sem levantar suspeitas.

2.6 Cultura dos usuários de não se preocuparem com segurança

Uma pesquisa feita pela empresa americana @Stake revelou que a principal causa de brechas de segurança é a falta de cultura sobre conceitos básicos de segurança [SEC 03]. O estudo descobriu que falta conhecimento dos usuários para mudarem esta cultura.

Mas é uma tarefa muito difícil atualmente gravar senhas, existe senha para o cartão magnético do banco, senha para acessar a conta bancária pela Internet, pelo telefone pode ser outra senha, senha de E-mail, senha da rede, senha do computador, senha da proteção de tela, senha da porta da sala dos servidores, e assim por diante, a tendência é as pessoas usarem a mesma senha para tudo ou escolherem senhas fáceis, ou ainda escreverem as senhas em algum lugar para não esquecerem.

Quanto as senhas de banco, já houve o tempo em que as pessoas andavam com a senha anotada junto do cartão, hoje ainda existe, mas é bem mais difícil, as pessoas tomaram conhecimento da importância do sigilo da senha. Mas, quando se trata de senha para acessos às informações da empresa a realidade é outra.

O usuário, na sua grande maioria, ainda não criou a cultura de se preocupar com a segurança das suas informações. É muito comum usuários com

senhas simples, como o seu próprio nome seguido de um número e quando o sistema obrigá-lo a trocar de senha ele apenas soma um a este número. Outros ainda deixam anotado a senha em um bloco de anotações, visível a todos [VIC 00].

Outra prática muito comum é o compartilhamento de senhas, uns emprestam suas senhas aos outros, dificultando a identificação efetiva dos usuários.

Além da despreocupação dos usuários com as senhas, existem outras culturas, como sair da sala e deixar o computador ligado e logado com a sua senha, não salvarem arquivos durante a digitação, freqüentemente, talvez por acharem que o sistema fará o salvamento sempre e que não haverá queda de luz, gravar arquivo nos diretórios locais de sua estação, mesmo sabendo que não existem backup da sua estação e mesmo o setor de informática orientando para gravarem apenas na rede, onde o backup é feito diariamente, e assim por diante.

Muitas destas culturas fazem parte da falta de conhecimento, o que novamente traz a tona o problema da falta de conhecimento citado no inicio deste capítulo.

2.7 Plano de continuidade de negócios inexistente ou nunca testado

Problemas de hardware e software podem acontecer todos os dias, muitas empresas podem ter medidas para disponibilizar novamente os sistemas após uma pane, uma falha no sistema, uma queda de luz, entre outros problemas, são poucas que ainda não se preocupam com estes incidentes e não possuem pelo menos uma medida de segurança para recolocar seus sistemas disponíveis em pouco tempo.

O grande problema é quando houver um incêndio, desastre, uma destruição total dos equipamentos ou da empresa, como no caso do World Trade Center. Outro exemplo é a empresa pegar fogo no final de semana, na segunda-feira, os funcionários chegarão para trabalhar aonde, o que fazer, ligar para quem? E se a empresa fica num local onde todos os acessos físicos foram interditados devido uma tempestade de muitos dias, os funcionários terão que ficar na empresa por um tempo indeterminado, a empresa tem condições de manter isso?

Mas pode acontecer também, da empresa possuir um plano de continuidade de negócios, muito bem organizado, descrevendo como reconstruir tudo no caso de um desastre, mas se este plano nunca foi testado, não é um plano confiável. Como saber se ele funcionará se nunca foi utilizado?

Numa das empresas em que a AUTORA trabalhou, houve um dia em tiveram que abandonar o prédio por causa de um princípio de incêndio, por sorte o incêndio foi contido pelos bombeiros rapidamente.

Mas, caso este o incêndio não tivesse sido contido, teria sido um desastre, a empresa possuía seguro dos equipamentos, mas todas as cópias de segurança dos sistemas, todos os relatórios, todas as informações da empresa de mais de 30 anos, dados de clientes, fornecedores, funcionários, tudo estava lá dentro e seriam transformados em cinzas em poucas horas. Quanto tempo levaria para esta empresa ser reconstituída? Será que seria possível?

2.8 Não existência de cópias de segurança das informações

É difícil encontrar alguém que não tenha perdido algum arquivo, por causa de falha de sistema, hardware ou queda de energia e que não tinha uma cópia atualizada do mesmo. Tem empresas prevenidas, que possuem sistema de cópias de segurança diário, mas se não for conferido diariamente, pode acontecer dele não estar sendo feito e isso só será notado do dia em que for necessário recuperar algum dado perdido.

Luiz Fernando Costa, ex-chefe da AUTORA, ensinou que, quem tem apenas uma cópia é o mesmo que não ter nenhuma, pois qualquer problema que houver, não tem como recuperar.

A própria AUTORA, no inicio da sua carreira nesta área, perdeu todos os dados de um sistema de um supermercado, com todos os produtos e seus preços, o relatório deste sistema era utilizado para serem colocados os preços nos produtos da loja. O backup estava desatualizado duas semanas, a alternativa foi baixá-lo e fazer todas as alterações de duas semanas manualmente, o que levou um dia de trabalho.

Infelizmente, algumas pessoas e empresas, precisam passar por prejuízos ou retrabalhos, para terem noção do quanto pode trazer aborrecimentos não ter uma cópia de segurança atualizada dos sistemas.

2.9 Uso de notebooks

A figura 2.1, mostrada no inicio deste capítulo, mostra o uso de notebooks como uma das ameaças, ele não chega a ser um grande problema para a maioria das empresas, mas cada vez mais se houve falar de notebooks roubados ou perdidos que continham informações importantes e sigilosas de empresas, isto caindo nas mãos erradas, podem trazer grandes transtornos e prejuízos. Portanto, o valor da informação contida em um notebook pode ser muito maior que o seu custo [RAB 00].

No informativo de segurança da Modulo, o Modulo e-Security News n° 188 [SEC 01], é publicado o desaparecimento de um notebook do ministério de

defesa britânico, contendo segredos de segurança nacional, depois que um oficial deixou o mesmo em um táxi. Em março de 2000 foi registrado que agentes dos serviços de segurança MI5 e MI6 perderam notebooks com dados confidenciais. Entre outros casos de roubo deste equipamento.

Segundo dados da pesquisa 2000 CSI/FBI Computer Crime and Security Survey, a soma dos prejuízos anuais de 1997 a 2000 resultantes do roubo de notebooks ultrapassa os 34 milhões de dólares [RAB 00].

Cada vez é mais comum as empresas adquirirem notebooks para facilitar o acesso às informações, na maioria das vezes são para utilização dos gerentes, diretores e demais cargos importantes na empresa, o roubo de um notebook com informações importantes pode trazer muito transtorno para as vítimas.

2.10 Pirataria

Pirataria é utilizar algo sem ter licença para isso. As empresas que possuem softwares instalados sem possuírem a licença para a utilização, estão ilegais e podem ser multadas por isso.

Algumas empresas não legalizam pelo alto valor destas licenças, outras, procuram legalizar tudo, mas precisam contar com o comprometimento dos seus usuários, pois é muito fácil copiar um programa, pegar um CD de instalação de

um software, com licença para uma máquina e instalar em várias. É difícil para a empresa controlar a ação dos funcionários, muitos softwares estão disponíveis na Internet para qualquer um copiar para sua estação e instalar.

Numa fiscalização, a empresa tem que prestar contas de todos os softwares instalados na empresa, o que não possuir licença a empresa tem que pagar multas altíssimas, gerando mais prejuízos do que se tivesse legalizado tudo.

Além da dificuldade com o controle de tudo que é instalado na empresa, a pirataria é um sério problema, pois o software pirata pode trazer falhas ou apresentar algum problema em que a empresa não terá como reclamar ao fornecedor, devido ao fato que não existe fornecedor.

3 MEDIDAS DE SEGURANÇA

3.1 Controle de acessos

Normalmente as organizações adotam medidas de segurança bem menos eficazes nos acessos internos, o que facilita as ações danosas, como descrito no capítulo 2, item 2.1.

Alberto Favero, Gerente de Auditoria de Sistemas na Área de ERS da Deloitte, numa de suas palestras [FAV 00], cita como alguns exemplos simples e eficazes conceder acessos somente a quem precisa, ter um procedimento para retirada de acessos quando da demissão ou transferência do usuário e parametrizar os softwares de acessos com tamanho mínimo de senhas, prazo de expiração de senhas e número máximo de tentativas inválidas antes de revogar o acesso.

Similar às dicas de Favero, uma prática simples e fácil de ser implantada em qualquer empresa é um controle de acessos, se a empresa possui

desenvolvimento próprio, pode solicitar que seja desenvolvido internamente um sistema para este controle, caso possua um desenvolvimento terceirizado, pode solicitar a compra, é um sistema simples que necessitará poucas horas de desenvolvimento.

Este sistema deverá ser acessado por todos na empresa, deve possuir um formulário de pedido de acessos, onde deve constar o nome do funcionário que receberá o acesso, o setor, telefone para contato e demais informações necessárias. Após estes dados devem constar os tipos de acessos existentes na empresa, onde o solicitante marcará quais o usuário necessitará, como acesso a rede, ao correio eletrônico, a Internet, etc. Para cada tipo de acesso, dependendo da característica dele, devem existir campos para maiores detalhes do acesso, e, por fim, deverá conter um espaço para a aprovação do gerente da área do usuário. O setor responsável por criar o acesso só o fará, após o pedido estar aprovado pelo gerente do usuário.

Está prática de controle de acessos com aprovação da gerência, foi criada pela AUTORA na empresa GKN do Brasil em 1999, e desenvolvido em Lotus Domino pela própria AUTORA, a idéia surgiu para solucionar problemas como os citados no capítulo 2 item 2.1, e também por que muitas vezes era concedido um acesso para um usuário e mais tarde o gerente do usuário cobrar, da área de informática, o motivo de ter dado o acesso, pois não deveria ter sido liberado. Este controle de acesso resolveu este tipo de problema, pois o gerente tem que

aprovar e assim, ele está ciente do acesso que será liberado para o seu funcionário.

Outra vantagem deste sistema é que ele mantém o histórico dos pedidos, quando foram solicitados, por quem, quem e quando aprovou, quando foi liberado, que acessos cada funcionário tem no sistema, o que facilita para uma auditoria assim como é uma segurança em caso de algum problema de perda de acessos no sistema, pois existe o histórico de quem acessa o quê.

Em empresas grandes, o ideal é que seja definido um facilitador de informática de cada área, este facilitador será o responsável por preencher o pedido de acesso sempre que um funcionário novo entrar no setor. Para o setor de informática em uma empresa grande é complicado conhecer tudo o que todos podem e devem acessar, já para o facilitador, que trabalha na área e está a par do que as pessoas na sua área precisam acessar, é bem mais simples.

Este facilitador deve ser treinado para isso. Muitas outras funções podem ser passadas para ele, sempre que for alterado algum sistema ou incluído alguma melhoria, pode ser repassado apenas para os facilitadores e estes se encarregam de divulgar para os seus colegas, facilitando assim a divulgação de informações dentro da empresa.

Usar facilitadores já é uma prática em muitas empresas grandes, um exemplo é a GKN do Brasil, que possui mais de 1200 funcionários, trabalhando em 3 turnos, o facilitador é peça fundamental para levar informações do setor de informática para as demais áreas como trazer informações, problemas e dúvidas das áreas para o setor de informática, sendo que alguns problemas simples de serem resolvidos, o próprio facilitador resolve, sem precisar da presença do técnico de suporte para isso.

Mas existem alguns acessos que, por se tratarem de acessos importantes, só devem ser liberados após treinamento, nestes casos o responsável por liberar o acesso deve ter um procedimento para controlar isso.

Mas, para o controle de acessos ser eficaz, deve existir um procedimento para retirada de acessos quando um usuário é transferido ou demitido. Se a empresa possui facilitadores nas áreas, eles podem ser os responsáveis por informar o setor de Informática quando isso acontecer. Mas no caso de demissão é necessário uma boa comunicação entre RH e Informática, para que faça parte do procedimento de demissão do RH, informar a Informática as demissões ocorridas, para que sejam removidos todos os acessos dos demitidos.

Mesmo com todos estes controles, pode acontecer de usuários solicitarem acessos e não utilizarem, uma maneira de conferir isso é verificado a data do último logon do usuário. Na rede netware é só entrar nas propriedades do usuário

que um dos campos mostra esta data. Numa rede NT, deve-se digitar o comando: “NET USER <login_do_usuário>” na console do servidor, aparecerão diversas informações do usuário, inclusive a data do último login do usuário. A AUTORA, ao fazer estas auditorias, removia todos os logins que o último acesso tinha sido há mais de 3 meses.

Estas práticas citadas acima ajudam a diminuir problemas de acessos indevidos internos e de ataques externos de ex-funcionários, assim como a utilização de sistemas importantes por pessoas sem o devido conhecimento.

3.2 Política de segurança

Andrea Thomé [THO 00], Consultora de Segurança da ISS, cita as pessoas, as métricas, políticas, padrões, procedimentos e controles adotados pela empresa, a monitoração, as ferramentas e os mecanismos bem configurados mais o treinamento e a conscientização dos funcionários como os responsáveis por garantirem a Segurança na empresa.

Segundo Thomé [THO 00], Política de Segurança pode ser definida como:

> “Um instrumento que contém diretrizes voltadas para auxiliar a Companhia no planejamento, definição e implementação de mecanismos (normas, procedimentos, padrões, controles e outros) que guiarão e suportarão as atividades que visem garantir a integridade, disponibilidade e confidencialidade das informações da Companhia”.

Numa pesquisa realizada pela ISS em dezembro de 1999 [THO 00] com 200 organizações, apenas 8% das empresas possuíam políticas de segurança implementada (escrita, formalizada e divulgada), 27% implantaram parcialmente e 65% das empresas não possuíam políticas de segurança.

O documento com as políticas de segurança de uma organização deve conter todas as normas, procedimentos e diretrizes da empresa que envolve a segurança das informações da empresa. Tudo o que a empresa dispõe de hardware e software e for liberado para a utilização dos funcionários, deve existir normas de utilização correta e segura e estas normas devem constar nas Políticas de Segurança.

Inclusive, deve ser estabelecido nas Políticas de Segurança as normas e procedimentos para utilização correta e segura de notebooks, laptops, palm tops, agendas eletrônicas, de papel e quaisquer outras formas de portar informações críticas dentro e fora da empresa [RAB 00].

Também deve estar bem definido quais são os direitos e os deveres dos usuários, ou seja, a responsabilidade de cada um. Uma boa Política de Segurança deve abranger aspectos sobre a confidencialidade das informações, a correta utilização das senhas e a punição para os usuários que não cumprirem as Políticas.

É importante ter um capítulo específico para terceiros e prestadores de serviços ou ser criado uma Política de Segurança específica para estes casos.

Durante o processo de elaboração das Políticas de Segurança da empresa deve existir o envolvimento do departamento jurídico e o apoio dos executivos da empresa.

Depois de finalizado a criação do documento deverá haver um controle de alterações ou versões, pois o mesmo deverá ser analisado pelo setor jurídico, pela gerência de informática e demais pessoas envolvidas com o processo na empresa como gerente de RH e Direção, de acordo com as normas da empresa, cada vez que passar por uma destas pessoas e houver alteração, altera-se o controle de versões.

Junto com as Políticas de Seguranças deve existir o Termo de Compromisso, com o nome do funcionário, descrevendo que ele está ciente das Políticas de Segurança, sabe das suas responsabilidades e concorda em cumprir o que está determinado. Todos devem assinar este Termo e quem não assinar deverá ter seus acessos cortados.

Após a implantação, as Políticas de Segurança devem fazer parte do procedimento de admissão do funcionário e serem entregues junto com o contrato de trabalho para o funcionário ler, aceitar e assinar. No caso de terceiros

ou prestadores de serviço, as Políticas de Segurança deverão ser entregues na contratação do serviço.

Para a implantação das Políticas de Segurança na empresa é necessário uma divulgação forte aos funcionários, terceiros e prestadores de serviços, a implantação pode ser total ou gradativa, dependendo da realidade de cada empresa. O grande problema é a aceitação das Políticas, pois para os funcionários, trata-se de novas regras e normas que, se não cumprirem, serão punidos e até demitidos.

Para isso não repercutir negativamente na empresa e quebrar a resistência dos funcionários, é necessário palestras explicativas e de conscientização sobre o assunto, mostrando estatísticas e exemplos sobre o assunto, para que todos entendam, apóiem e se comprometam com o processo. O objetivo é trazer o funcionário para ser um parceiro da empresa neste processo.

Após a implantação, segundo Lorenzo Ridolfi, Diretor de Negócios da Choice [RID 00], o processo deve ser sempre acompanhado por responsáveis do setor de informática, sempre que houver necessidade, deve ser atualizado e monitorado. Se não forem criados procedimentos para controlar se as Políticas estão sendo seguidas pelos usuários ou não, os procedimentos das Políticas

acabam no esquecimento, por isso a necessidade da monitoração através de Auditorias Permanentes, conforme será descrito no item 3.3..

A Política de Segurança implantada, monitorada e mantida, ajuda a minimizar os problemas de Acessos Indevidos internos, Vírus, Pirataria e Falta de Cultura dos usuários de não se preocuparem com segurança e a utilização de Notebooks.

3.3 Auditorias permanentes

Não basta a criação e implantação das Políticas de Segurança em uma empresa se não existirem mecanismos de controle, para assegurar que a Política de Segurança será seguida. Uma das maneiras de controlar tudo isso é através de auditorias permanentes.

Uma auditoria envolve profissionais especializados da área de informática, que irão sortear alguns funcionários e fazer auditorias de detecção dos desvios na política nos acessos e na utilização dos recursos por estes funcionários. Deve ser permanente, pois quando a auditoria não for freqüente as incidências de desvios no cumprimento das políticas aumentam. Infelizmente, a maioria dos usuários só respeita, quando sabe que poderá ser descoberto e punido por isso.

Deve-se ter bem claro o que será auditado e as punições para cada tipo de não-conformidade com as normas da empresa. Geralmente, os itens mais importantes a serem auditados são a utilização do correio eletrônico, acessos à Internet, arquivos gravados na rede e nas pastas locais das estações dos usuários, se os acessos que o usuário possui estão de acordo com a função dele na empresa, entre outros, de acordo com os recursos disponibilizados pela empresa.

A pessoa responsável pela auditoria deverá fazê-la da maneira mais sigilosa possível, não pode vazar o que for encontrado durante a auditoria, é uma tarefa muito difícil, pois a pessoa que fizer estas auditorias pode ser ameaçada por colegas ou sofrer indiferenças por causa disso. Os auditores passam a atuar como consultores, utilizando suas habilidades tradicionais para reconhecer e solucionar problemas.

A AUTORA fez parte do grupo que desenvolveu o procedimento de auditoria na GKN do Brasil e foi escolhida para ser a auditora. Foi desenvolvido um sistema em Access por um de seus colegas, que buscava todos os logins da rede e sorteava 20. Mensalmente este sistema era rodado e era feita a auditoria dos 20 usuários sorteados. Era uma tarefa crítica, demorada e constrangedora.

No final da auditoria deve ser elaborado um relatório com todas as não conformidades encontradas e demais informações importantes, para ser

entregue a Gerência de Informática ou outra pessoa de acordo com as características da empresa.

Deve-se notificar o usuário que fere as normas das Políticas de Segurança da empresa, para que ele procure mudar a sua atitude e saiba que, se caso venha acontecer novamente, ele receberá uma punição mais grave.

De acordo com pesquisa realizada pela empresa Quick Take [SEC 02], o que leva os executivos monitorarem a utilização do E-mail e da Internet, para 54% dos entrevistados é pelo aumento da segurança, enquanto que para 20% é pelo aumento da produtividade. Nesta pesquisa foram entrevistados executivos de Informática e usuários e mostrou que 75% dos entrevistados concordam com a adoção de práticas para a monitoração de utilização da Internet. E muitos executivos admitiram que já utilizam estas práticas.

As auditorias permanentes também ajudam a minimizar os problemas com acessos indevidos, mas o objetivo principal é monitorar se as políticas de Segurança estão sendo seguidas, auxiliando assim, que os problemas minimizados pelas Políticas de Segurança implantadas continuem a ser minimizados.

3.4 Política de Backup´s

Essa medida é essencial para a continuidade dos negócios da empresa, todas as informações e sistemas da empresa necessitam ter cópias o mais atualizadas possíveis para a recuperação destas informações caso seja necessário.

No livro Vivendo a Segurança da Informação, Fontes [FON 00] diz que “um plano de cópias de segurança tem por objetivo suprir a empresa quando for preciso recuperar dados de épocas passadas”.

Existem no mercado diversos softwares de backup, a empresa deve escolher o que melhor se adequar às soluções da empresa e deve treinar e preparar pelo menos duas pessoas para serem responsáveis pelo processo de backup e restore.

Um procedimento correto de backup deve ser definido por pessoas chaves dentro do setor de informática, onde deve ser definida a periodicidade em que os backups serão feitos, o ciclo de existência das cópias, dados a serem copiados e quanto, pois as informações que são alteradas diariamente como arquivos gerais e correios eletrônicos dos usuários, devem possuir backups diários, já os sistemas operacionais, demais softwares utilizados na empresa, configurações de cadastros de usuários podem passar por backup semanais.

Além disso, deve ser previsto local para armazenamento das cópias de backup, a sugestão é que este local seja diferente do local onde estão localizados os servidores, pode ser em outro setor da empresa ou outra filial e que sejam armazenados dentro de um cofre, de preferência. Uma atitude profissional da empresa é manter uma cópia atualizada de tudo em um local externo, demonstrando seriedade com que ela trata as suas informações.

Após cada backup deve ser feito um procedimento para verificação do backup, deve ser revisada a consistência do backup, se ele realmente rodou, se não deu nenhuma mensagem de erro, entre outras verificações. O ideal é a verificação não ser feita pela mesma pessoa que fez ou disparou o procedimento de backup, pois quem fez pode achar que fez tudo correto e não fazer a verificação.

Possuir cópias de segurança atualizadas e íntegras exige profissionalismo e responsabilidade e todo o processo de recuperação de informações é importante para o negócio da empresa e até mesmo para a continuidade da organização.

Para garantir que os dados do backup são válidos, é aconselhável que seja recuperado algum arquivo para testar a integridade do backup.

Esta medida ajuda e evitar os problemas por falta de cópias de segurança no caso de falhas, que foram detalhados no capítulo 2.

3.5 Treinamento e disseminação do conhecimento

No livro Segurança Máxima [XIM 00] o autor coloca a educação dos usuários como a melhor política para as empresas alcançarem pelo menos uma segurança mínima. Segundo ele, o que for gasto agora poderá economizar muitas horas no futuro, fazendo com que está prática também seja econômica.

Para uma utilização correta e configuração ideal de softwares e hardwares uma empresa precisa de profissionais especializados ou treinar os seus funcionários para esta tarefa. Pode treinar um ou dois e estes repassarem seus conhecimentos aos demais.

Uma prática que traz bons resultados é sempre possuir no mínimo uma pessoa especialista em cada sistema e recurso utilizado na empresa, e sempre ter no mínimo duas pessoas responsáveis por cada sistema, com conhecimento suficientes para resolverem os principais problemas, em caso de falta do especialista.

Dentro desta prática de treinamento e disseminação de conhecimentos também entra o usuário final. É preciso treinar o funcionário para todos os

sistemas e recursos que ele for utilizar. A melhor maneira de fazer isso depende da realidade de cada empresa. Isso é mais uma função do setor de treinamento da empresa do que do setor de informática, mas o setor de informática tem a responsabilidade de acompanhar este processo para certificar que ele realmente está acontecendo.

Os funcionários novos podem ser treinados por funcionários mais antigos, ao disponibilizar novos recursos, a área de informática tem que prever tempo, pessoas e material e local para o treinamento dos funcionários que irão interagir com este novo recurso. Quem sabe, ou que foi treinado para determinado recurso, pode replicar seus conhecimentos aos demais colegas que conhecem menos ou nada a respeito, não precisa ser apenas num treinamento, auxiliar o colega ao lado é uma prática muito eficiente.

Todo o processo deve envolver pessoas das áreas afetadas. Uma metodologia que costuma funcionar é criar ciclos de palestras onde toda a documentação é apresentada de uma forma clara e interessante ao público. Tirar os nomes técnicos e apresentar como uma seqüência, uma estória, onde a segurança da informação é o protagonista, são adaptações das metodologias utilizadas em treinamentos de segurança do trabalho, e que funcionam.

Treinar os funcionários e fazer com que todos repliquem seus conhecimentos irá minimizar problemas de vulnerabilidades de software, pois o

usuário com mais conhecimento a respeito das vulnerabilidades irá se manter atualizado sobre as vulnerabilidades dos sistemas utilizados na sua empresa para instalar as soluções sempre que disponíveis.

Também minimizará os problemas citados sobre a falta de conhecimento dos usuários, por terem mais conhecimento não serão ingênuos ao receberem arquivos que possam conter vírus, além de que diminuir os problemas de Pirataria de software, pois uma vez consciente dos problemas que isso pode ocasionar irá ajudar a empresa no controle destas piratarias.

3.6 Atualização e legalização de softwares

Esta medida tem como objetivo elaborar um procedimento para controle de licenças, além da atualização dos softwares.

Para isso a empresa deve manter atualizado o seu inventário de máquinas e os softwares instalados. O ideal é que este inventário seja feito automaticamente através de softwares existentes no mercado, mas a maioria destes softwares são muito caros e as empresas optam por não utilizá-los, o que torna este trabalho mais difícil e menos eficaz, pois o inventário tem que ser feito manualmente, máquina por máquina, ocupando muito tempo dos profissionais.

Além disso, este sistema precisa estar sempre atualizado, como é feito manualmente precisa de um comprometimento muito forte dos responsáveis por este controle.

Quanto a atualização de software, cada técnico de informática deve ser responsável por manter atualizado o seu sistema, pesquisar sobre possíveis vulnerabilidades e novas versões ou soluções disponíveis e sempre atualizar seu sistema, ou também a empresa pode ter uma pessoa responsável por cuidar da atualização de todos os sistemas, esta decisão depende da realidade de cada empresa.

Esta prática visa minimizar os problemas de vulnerabilidades e de pirataria de softwares.

3.7 Atualização de Antivírus

A proposta aqui é criar um procedimento para que exista um sistema de antivírus instalado, ativado e atualizado em todos os computadores da empresa.

Primeiramente é necessário que dentro do setor de suporte da empresa sejam destinadas duas pessoas como responsáveis deste processo. A empresa precisa possuir um sistema de antivírus para os seus servidores e todas as estações de trabalho, que seja configurado para ficar sempre ativado, assim

qualquer arquivo aberto que esteja com vírus o antivírus irá avisar. Também é necessário um software de antivírus para o correio eletrônico, este software verifica mensagens por mensagens detectando se existe algum arquivo com vírus anexado.

Após a instalação dos antivírus em todos os sistemas é necessária a monitoração, das pessoas responsáveis por este processo, no que diz respeito a atualização dos antivírus, todo o dia surgem novos vírus e com eles as atualizações dos antivírus, é preciso estar atento aos fornecedores dos softwares comprados, geralmente as atualizações são disponibilizadas na Internet, basta baixá-las para os servidores e após, atualizar as estações de trabalho.

Este processo citado acima pode ser automatizado com algumas rotinas de execuções que façam parte ou todo este processo sozinhas e apenas sejam monitoradas pelos responsáveis. Por exemplo, ao buscar o arquivo com a nova versão do antivírus, pode ser executada uma rotina que instale esta nova versão em todos as estações da rede através do login do usuário.

3.8 Plano de continuidade de negócios

O plano de continuidade de negócios ou plano de contingência é um procedimento contendo ações para a continuidade do negócio, em caso de contingência.

Um plano de contingência é um mecanismo de segurança, explica em Fernando Saldanha em um dos seus artigos [SAL 00], onde deve constar a definição do escopo, a identificação dos desastres e ameaças e a seleção das estratégias.

Um plano de contingência deve possuir ações que garantam que os processos que permitem a realização do negócio vão continuar acontecendo, apesar de ter ocorrido uma situação de contingência [FON 00]. A solução deve contemplar todos os elementos necessários para isso tanto técnicos como humanos. Por exemplo, algumas das empresas que possuíam filiais no World Trade Center, mesmo com planos de contingências tiveram dificuldades em restabelecer seus sistemas por que as pessoas envolvidas haviam desaparecido.

A criação do plano de contingência começa pela definição do escopo, onde se deve contemplar todas as áreas, todos os recursos, todos os sistemas da empresa, além de considerar também os aspectos geográficos, tecnológicos e funcionais. Uma ferramenta para este trabalho é a Análise de Impacto de um Desastre, que consiste num método para identificação das perdas por causa de paralisação de um processo de negócio, em cima destas perdas deve-se identificar o nível de criticidade de cada processo e a sua prioridade.

A segunda etapa é identificar quais desastres a empresa está exposta como falta de energia elétrica, vendavais, enchentes, terremoto, incêndio, greve

de funcionários ou de outros sistemas que podem indiretamente afetar o negócio da empresa, como greve de caminhoneiros, transportes em gerais ou fornecedores. Esta atividade pode ser feita através da Análise de Risco.

A elaboração do plano de contingência compreende o detalhamento do que será feito, por quem será executado, como estas pessoas podem ser encontradas, onde estão as mídias e demais recursos necessários para cada execução. E o documento completo do Plano de contingência deve ser sempre atualizado e ficar em local de fácil acesso. Assim como, deve existir cópia dele em algum local fora da empresa.

Segundo Fernando Saldanha [SAL 00], para a implantação do Plano de contingência deve haver antes um treinamento de todos os envolvidos, a contratação de serviços, assim como a compra e a instalação dos recursos necessários para a implantação e testes do plano. Um plano não testado ou desatualizado pode trazer tantos problemas para a empresa quanto a não existência de um plano.

O plano de continuidade de negócios é um conjunto de ações e só será eficaz se estas ações não forem consideradas isoladamente e se este plano for testado freqüentemente.

Com esta medida se propõe evitar problemas referentes a não haver plano para a continuidade do negócio ou plano para situações de risco na empresa.

3.9 Firewall

A instalação do Firewall é crucial para a empresa garantir controles mínimos dos pontos de entrada e saída da suas rede, onde o Firewall irá selecionar, permitindo ou bloqueando, as conexões que poderão passar [PAU 00].

Para a implantação do Firewall a sugestão é a contração de pessoas ou empresas especializadas, para evitar problemas como os mencionados por falta de conhecimento, no capítulo 2. A configuração deve ser feita de forma a permitir as funcionalidades necessárias, que empeçam um ataque externo tenha acesso à rede local [PAU 00]. Uma metodologia eficaz é bloquear tudo e criar regras apenas para os acessos permitidos.

3.10 Segurança na Sala dos Servidores

A sala dos servidores é o coração tecnológico da empresa. Este local deve ficar restrito apenas aos técnicos de informática responsáveis pelos

servidores. Qualquer comando executado de maneira incorreta num dos servidores, pode ocasionar uma indisponibilidade nos serviços. Até mesmo para limpeza da sala, o ideal é que um técnico acompanhe a equipe de limpeza para não tocarem nem desligarem nenhum equipamento.

Numa empresa onde a AUTORA trabalhou, numa destas limpezas, que na época não eram acompanhadas por um técnico, a faxineira simplesmente desligou um dos cabos de força de um dos servidores para ligar o aspirador de pó. Em outra circunstância, um estagiário, procurando um local para ligar o cabo de aquecer água quente, colocou num dos no-breaks dos servidores, como o no-break estava quase no máximo e como a resistência para aquecer água puxa muita energia, o no-break não deu conta e acabou desligando tudo, inclusive os servidores.

4 IMPLANTAÇÃO DAS MEDIDAS DE SEGURANÇA EM UMA EMPRESA DE GRANDE PORTE

4.1 Quadro inicial

A AUTORA começou a trabalhar nesta empresa em dezembro de 1998, como analista de suporte e entre as suas responsabilidades estava a administração da Rede, administração do Correio Eletrônico e atividades de suporte a software em geral.

Não estava embutido nas funções da AUTORA, tarefas de segurança, mas isto já era uma preocupação da mesma, que começou a analisar o quadro e encontrar muito focos de falhas em segurança.

Alguns exemplos disso são, a senha do administrador de toda a rede não era trocada freqüentemente e além do setor de informática, referenciado a partir de agora por DTI, várias pessoas de outras áreas possuíam acessos, como

funcionários da engenharia e do RH. Retirar a posse da senha do administrador destes usuários e deixá-la apenas com os administradores da rede foi a primeira grande tarefa da AUTORA.

Ao analisar os logins, foram encontrados mais de 900 logins cadastrados, muitos de funcionários demitidos e até mesmo logins duplicados, ou seja, como não era seguido um critério rígido para a criação de logins, poderia acontecer de criarem dois logins para a mesma pessoa.

Também não existia um controle de solicitação de acesso, o próprio usuário ligava e solicitava o que queria por telefone o acesso era liberado.

Não existia política de segurança, funcionários possuíam jogos instalados, copiavam softwares de um micro para o outro, traziam de casa e instalavam sem o conhecimento do DTI, desconfiguravam softwares já configurados, trazendo diversos problemas.

Além disso, existia muita reclamação dos usuários quanto a demora dos técnicos em atenderem seus problemas, já que muito tempo era perdido por falta de organização, controle e retrabalhos. Foi então que a AUTORA, junto com seus colegas do DTI começaram a montar um plano de ação para os problemas encontrados.

4.2 Controle de Acessos

O primeiro passo dado pela AUTORA foi alterar a senha do administrador, apenas os administradores de rede souberam da nova senha e tinham ordens para não passar a ninguém. As pessoas que ligavam, por não conseguir acessar a senha do administrador tinham os seus acessos alterados para poderem realizar o que necessitavam sem usar a senha do administrador e, assim, qualquer problema que viesse a acontecer, seria mais fácil a identificação do autor. A senha do administrador passou a ser alterada mensalmente, utilizando senhas com a mistura de letras e números.

Em seguida, a atenção da AUTORA foi para os logins cadastrados na rede, a tarefa foi fazer uma análise geral em todos os logins. Na época a rede era Novell, todos os logins com data de último logon anterior há 3 meses foram removidos. Nesta limpeza foram removidos mais 200 logins.

O próximo passo foi a implantação de um controle de acesso, conforme descrito no capítulo 3, item 3.1. A AUTORA desenvolveu em Lotus Domino um sistema para controle de acessos. A partir do momento que foi implantado, todos os pedidos de acessos tinham que ser feitos por este sistema e com a aprovação do gerente do usuário.

Com isso, solucionaram-se vários problemas, mas ganhou-se muito em produtividade, pois o acesso criado era conforme a solicitação, não tinha problemas dos técnicos esquecerem de criarem o acesso, pois estava no sistema. E também não ocorriam problemas de nomes escritos errados, pois o nome era digitado de acordo com o crachá do solicitante no formulário e não por telefone. No Anexo I está uma cópia do formulário de pedido de acesso utilizado na empresa.

4.3 Política de Segurança

No final de 1999 foi formado um grupo de técnicos do DTI, entre eles estava a AUTORA, para inicio da elaboração das Políticas de Segurança. Na época as políticas já haviam sido implantadas na matriz da empresa nos Estados Unidos e este grupo começou a estudar como implantar estas Políticas nesta filial.

O primeiro passo foi determinar todos os recursos disponibilizados pela empresa aos seus funcionários e quais as regras de utilização para cada recurso. Para cada um foi detalhado a descrição, composição e demais características.

No recurso ambiente de rede, foi descrito também como acessá-lo, regras de senhas, proteção contra perdas, confidencialidade das informações, retenção

de registros, com dicas para limpeza freqüente dos registros e espírito de equipe, onde se solicitava e disseminação dos conhecimentos.

Outros recursos detalhados na Política são Proteção contra vírus, utilização de Modens, pois pelas normas da empresa, as estações não devem ter modem, mas como alguns softwares necessitam desta configuração, foi detalhado na Política que ao utilizar um Modem em uma estação, a mesma deve estar desconectada do ambiente de rede.

Foram detalhadas também o uso da Internet, do Correio Eletrônico e demais softwares utilizados na empresa, com destaque sobre Pirataria de software.

Após, para a elaboração propriamente dita, houve a participação do departamento jurídico da empresa, que pode ajudar dando os detalhes legais para a criação das Políticas.

Com o documento pronto, ele foi passado para a analise final do Gerente de Informática, depois pelo Setor Jurídico, após pelo Gerente de RH e por último pelo Presidente da empresa. Após todas as alterações sugeridas feitas, o documento estava pronto para ser implantado.

Para a implantação, houve palestras de divulgação e explicação a todos os usuários, principalmente os facilitadores, pois eles seriam os responsáveis por repassar aos que não pudessem participar das palestras. O objetivo destas palestras era conscientizar os usuários da importância das Políticas e da participação de deles no processo.

Após, as palestras, foram entregues as Políticas para cada área, os funcionários leram, assinaram o Termo e devolveram apenas o Termo de Compromisso para o Departamento Pessoal (RH), que foi anexado à pasta pessoal de cada funcionário no RH. Foi dado um prazo de 2 meses, os funcionários que não assinaram o Termo dentro deste prazo, tiveram seus acessos cortados.

Parte do documento com as Políticas de Segurança da empresa podem ser vistos no Anexo II. Por ser um documento sigiloso da empresa, só foi possível incluir partes do documento que foram liberadas pela empresa.

Nestas políticas não está descrito sobre as normas corretas e seguras de utilizar notebooks, laptops, palm tops e agendas eletrônicas, pois estes recursos não eram utilizados pela empresa para armazenamento de informações, apenas os notebooks eram utilizados, mas para apresentações em salas sem estações de rede.

Assim que foram comprados notebooks e laptops para utilização de gerentes foi criado um Termo de Compromisso para a utilização deste tipo de recurso e assinado por cada usuário que recebia o recurso.

Este termo também foi utilizado para os usuários que possuíam palm tops particulares, pois no inicio a empresa não queria liberar a entrada de palms particulares na empresa, mas depois, decidiu-se por incluir na norma de utilização, já que é uma ferramenta útil.

4.4 Auditorias

Após as políticas implantadas, o próximo passo era a auditoria, para a verificar se as políticas estavam sendo cumpridas. A AUTORA junto com o Gerente da área e mais um colega, montou o procedimento para execução da auditoria, onde consta o que será auditado, qual a periodicidade e qual a punição aos infratores.

Decidiu-se por verificar todos os acessos de rede, se caso o usuário sorteado tiver acesso a Internet, seria verificado o log dos acessos dele na Internet, a caixa postal dele, onde seriam verificadas as mensagens, se ele recebe ou envia mensagens que não são referentes a trabalho, etc. Além de ser auditado o micro onde o usuário trabalha e seus acessos no sistema de ERP da empresa.

Na primeira auditoria feita, foram encontradas diversas não conformidades, entre elas fotos de pornografia em computadores da empresa e em diretórios da rede, e-mails com arquivos anexados sendo enviados por funcionários da empresa com assuntos pornográficos, piadas, correntes entre outros. No Anexo III está uma parte do procedimento de auditoria e no Anexo IV, um exemplo de um dos relatórios finais de auditoria feito pela AUTORA. Por ser um documento sigiloso da empresa, não foi possível colocar o procedimento de auditoria na íntegra em Anexo.

Seguindo as regras de punições definidas, houveram usuários com acessos de correio eletrônico cortado por um período, outros receberam advertências verbais ou escritas e alguns foram demitidos.

Os casos de demissões foram por acessos constantes a sites de nudismo, pornografia e pedofilia.

Para geração do Log de acessos à Internet de cada usuário utilizou-se o software WebTrend Firewall Suite, ele gera todos os acessos por usuário por período, mostra percentual de acessos de cada site e tempo utilizado. Por exemplo, um dos usuários punidos, no Log dos acessos dele na Internet, mostrava que ele utilizava em torno de 10 horas semanais em sites de classificados de empregos e sites de entretenimento em horário de trabalho.

Mais detalhes no site www.clm.com.br/webtrends, em produtos/firewallreporting/fs/default.asp.

Para pesquisa de arquivos indevidos, pode ser utilizados os recursos de pesquisa dos próprios sistemas operacionais. Mas a grande parte da auditoria pode ser feita manualmente, ou seja, abrindo-se arquivos suspeitos, entrando na caixa postal do usuário e verificando o conteúdo das mensagens com assuntos suspeitos.

Além disso, registro e análise de logs são preciosas ferramentas em processos de auditorias. Pois os logs trazem inúmeras informações que se transformam em indicadores capazes de medir os níveis de segurança e de avaliar se medidas de segurança estão surtindo o efeito esperado.

4.5 Política de Backups

Para a elaboração das políticas de backup, também foram definidas algumas pessoas para compor a equipe responsável por este projeto. Na verdade a empresa já possuía uma rotina de cópias de segurança, mas no momento de criar a Política de Backup, muita coisa foi reconsiderada.

A empresa havia migrado sua rede Netware para uma rede NT, o backup somente seria feito dos arquivos existentes em pastas da rede e não de arquivos gravados localmente nos micros. Os usuários sempre foram avisados disso.

A primeira etapa da elaboração desta política foi a definição do que necessitava de backup, por exemplo, os arquivos dos usuários, os sistemas de ERP, configurações de sistemas operacionais, entre outros. Após foi a vez de definir a periodicidade de backup de cada dado a ser copiado. A AUTORA foi responsável por determinar as necessidades dos arquivos de usuários e sistemas gravado na rede NT e de todo o sistema de correio eletrônico que eram os sistemas que a AUTORA administrava.

Por exemplo, os sistemas de ERP, que constam dados de compras, contas a pagar, contas a receber, estoque, planilhas de MRP e demais planilhas de produção da empresa devem ter backups diários. Assim como os arquivos dos usuários gravados na rede e as caixas postais do sistema de correio eletrônico. Estes foram definidos para sofrerem backups diários totais, backups semanais e mensais,

Já as configurações de sistemas operacionais de servidores, como não eram alteradas todos os dias, iriam sofrer backups semanais e mensais.

Assim foi feito para cada informações que deveria sofrer backup. No final foi criada uma tabela onde foi listado o que deveria ser copiado e para cada um definido a periodicidade das cópias, de quanto em quanto tempo seriam copiados, por exemplo, a cada 24 horas, a cada 7 dias.

Outra definição importante foi o tipo de backup, se Full ou Incremental, no Full é copiado tudo enquanto que no Incremental é copiado apenas o que foi alterado desde a última cópia, por quanto tempo deve ser preservada a cópia, 7 dias, 1 mês, 5 anos e a média de espaço necessário.

Tudo isso faz parte do procedimento de backup, conforme pode ser visto detalhadamento nos Anexo V e VI. Onde consta uma cópia dos procedimentos e das rotinas de Backup da empresa.

4.6 Treinamento e Disseminação de Informações

Paralelo a isso, a equipe de suporte do DTI começou a se reestruturar, enquanto antes todo mundo fazia tudo, começaram a deixar cada um com as atividades de suas habilidades e preferências, o que contribui para que cada um se especializasse na sua área.

A AUTORA sugeriu a realização de uma reunião semanal da equipe para troca de experiências e informações, esta idéia foi aceita por todos e implantada

imediatamente. O resultado é positivo e deixa todos a par de tudo que está acontecendo no setor, além da troca de conhecimentos.

Foram montados treinamentos, de softwares utilizados na empresa, para que todos pudessem se inscrever, e os instrutores foram os próprios técnicos de informática. Isto é uma política da empresa em geral, onde os funcionários repassam suas especialidades através de cursos para os demais colegas. Cada hora de curso dada reverte em hora de treinamento para o instrutor receber.

E para todas as tarefas realizadas pela equipe foram criados procedimentos passo-a-passo para documentação das atividades. Por exemplo, em caso das pessoas responsáveis pelo backup não estarem na empresa e ser necessário fazer uma cópia urgente de algum arquivo, um outro técnico, através dos procedimentos, poderia realizar. Claro que algumas tarefas mais complexas era dado um treinamento básico para os demais colegas.

4.7 Atualização e Legalização de softwares

Os técnicos já divididos em suas áreas de atuação se tornaram responsáveis pela atualização dos softwares da sua área. Além disso, eles devem sempre se atualizar, procurando novas tecnologias que possam trazer melhorias aos sistemas já utilizados na empresa ou novas tecnologias para propiciar melhoramentos nas diversas áreas da empresa.

Esta atualização é feita através de leituras de revistas especializadas sobre o assunto, pesquisas na internet, participações em feiras, eventos e congressos. No Anexo VII existe uma relação de sites sobre o assunto.

Quanto a legalização, foi desenvolvido em Visual Basic pela AUTORA, como trabalho da cadeira de Linguagem de Programação I, um sistema para controle de recursos que permite o cadastro de máquinas da empresa, softwares instalados nas máquinas e licenças existentes. A AUTORA implantou este sistema na empresa, que possibilita a importação de dados do SMS, software da Microsoft para fazer o inventário de máquinas e softwares das estações da rede.

Como a empresa decidiu por não comprar o SMS, devido ao alto custo do software, os técnicos de suporte tiveram que começar com um mutirão, para fazer manualmente este inventário de todas as máquinas da empresa e softwares instalados em cada máquina. Após, estes dados inventariados foram digitados no sistema de Controle de Recursos, desenvolvido pela AUTORA. Paralelo a isso, foi feito um levantamento de todas as licenças existentes na empresa, que também foram cadastradas no sistema.

Com tudo cadastrado, a tarefa foi cruzar os dados, através de visões específicas do sistema, onde foi possível verificar as licenças que deveriam ser compradas e o número de licenças de cada software que estavam sobrando.

A empresa já possuía um controle rígido de instalações de licenças Microsoft, no qual possui contrato Select e a cada 3 meses reportava as novas licenças instaladas. Neste caso, no que se refere a Microsoft, as instalações que foram encontradas que ainda não possuíam licenças, foram reportadas período seguinte. Quanto as demais necessidades encontradas foram iniciados processos de compras para elas.

A partir dai, toda nova instalação de software precisa ser solicitada pelo usuário através do sistema de Solicitação de Recurso, desenvolvido pela AUTORA em Lotus Domino, onde o usuário deve descrever o software que ele necessita que seja instalado, o número da máquina (estação) onde deverá ser instalado e o motivo. Após a criação desta solicitação o gerente do usuário deve aprovar e depois vai para a aprovação do gerente do DTI.

Apenas após a aprovação do gerente do DTI é que o suporte irá fazer a instalação, se houver licença para isso, senão, será primeiramente comprada a licença e após será feita a instalação e atualizado o sistema de Controle de Recursos.

4.8 Atualização de Antivírus

Como nas outras medidas, esta medida também foi implantada por um grupo de técnicos do suporte com a participação da AUTORA.

O antivírus escolhido para os servidores foi o Norton Antivírus, este antivírus já havia sido escolhido pela empresa antes da AUTORA fazer parte da equipe de suporte.

Nos procedimentos de instalações de uma estação, um dos requisitos é a instalação do antivírus local, que deve ficar ativado sempre que a máquina for ligada. Os antivírus existentes no mercado possuem esta característica.

No caso do Norton Anivírus, escolhido pela empresa, ele possui um recurso chamado Liveupdate, onde é configurado de quantas em quantas vezes por semana o sistema deve verificar se existe atualização. O próprio Liveupdate vai ao site da Symantec, fornecedor do Norton, se existe atualização ele atualiza o sistema da empresa.

Os softwares que não possuem este recurso, o próprio técnico deve criar um procedimento para, pelo menos duas vezes por semana, verifique se existem atualizações e atualize seus servidores e estações de trabalho.

A atualização nas estações, nesta empresa, é feita através de uma rotina BAT que executa através do logon do usuário. Mesmo assim, sempre que possível e verificado se as estações estão com o antivírus atualizado e ativo, geralmente isto é verificado quando um técnico vai resolver algum problema na

máquina ou é solicitado para que os facilitadores de cada área observem suas estações e avisem sempre que encontrarem alguma irregularidade.

4.9 Plano de Continuidade de Negócios

O plano de continuidade de negócios desta empresa foi elaborado com a participação de dois técnicos de suporte, sendo a AUTORA e mais um colega, o chefe da área de suporte e em algumas decisões importantes, o Gerente do DTI.

A matriz da empresa nos EUA já possuía um Plano de continuidade de negócios, e foi utilizado o plano da matriz como base para a criação do plano aqui no Brasil.

A elaboração do plano de contingência começou pela definição do escopo, onde foi verificado todos os recursos, todos os sistemas da empresa, além de considerar também os aspectos geográficos, tecnológicos e funcionais. Isto foi feito através da ferramenta Análise de Impacto de um Desastre, onde foi identificado todas as perdas por causa de paralisação de um processo de negócio.

Após esta identificação, foi o momento de levantar o nível de criticidade de cada processo e a sua prioridade.

A próxima fase foi a identificação de quais desastres a empresa está exposta através da Análise de Riscos, onde foram identificados a falta de energia elétrica, vendavais, enchentes, incêndio, greves de funcionários ou de outros sistemas que podem indiretamente afetar o negócio da empresa.

Após, foi definido as responsabilidades de cada pessoa e cada um ficou responsável por detalhar a sua parte, com detalhes técnicos de como será feito a reinstalação ou configuração do sistema ou recurso, quais pessoas que podem ser contatadas (sempre tem que ter no mínimo duas pessoas aptas), como estas pessoas podem ser encontradas, onde estão as mídias e demais recursos necessários para cada execução. Nesta etapa a AUTORA ficou responsável de descrever todas as necessidades para estabelecer novamente a rede e o correio eletrônico, no que se refere ao sistema operacional, arquivos, contas de usuários, configurações, instalação dos softwares necessários entre outros itens.

Após o documento estar pronto, foi definida uma data para testar a funcionalidade, ou seja, o plano foi testado com a simulação de um desastre, onde foram identificados algumas falhas e alguns itens que haviam sido esquecidos. Depois do plano de contingência completo foi definido que a cada dois meses ou quando houver alguma alteração o plano será revisado e a cada 6 meses testado novamente.

Existe cópia do plano na rede, em disquete e impresso. Sendo que uma cópia impressa fica num cofre existente no Departamento de RH e uma no cofre existente na filial em uma cidade vizinha. Existem também, cópias das mídias para instalação dos sistemas nos dois cofres citados acima.

4.10 Implantação do Firewall

A empresa implantou um Firewall para obter segurança principalmente no controle de acessos externos à empresa, poder bloqueador os acessos indevidos e possuir medidas para minimizar os ataques de hackers de crackers.

A empresa fornecedora do firewall foi contratada para fazer a instalação e configuração e também para dar treinamento aos técnicos sobre o Firewall. A AUTORA acompanhou a implantação, recebeu um treinamento básico para as configurações, mas, como as duas pessoas escolhidas para serem as responsáveis pela configuração do Firewall foram as pessoas que cuidam da parte de comunicação e sistema físico da empresa, a AUTORA, não participou da continuação do processo.

Mas foi possível, durante o período inicial, perceber a infinidade de configurações possíveis, um firewall bem configurado pode impedir ataques DoS, impedir que hackers acessem máquinas internas, filtrar os acessos dos funcionários a sites não permitidos pela empresa, entre muitos outros recursos.

Além disso, tudo que acontece fica registrado no Log e é possível gerar relatórios de diversas maneiras referentes aos acessos permitidos ou bloqueados, data, quem acessou, entre outras informações.

4.11 Segurança na sala dos servidores

Na porta de entrada da sala dos servidores, for instalada uma trava com senha, onde, apenas os técnicos responsáveis pelos servidores possuem a senha para entrar, sendo que aos finais de semana a senha é outra e esta é restrita a apenas dois técnicos, que são responsáveis pelo backup e ao chefe do setor.

Além disso, a senha cadastrada tem prazo de expiração, a cada mês elas são alteradas e se algum dos técnicos trocarem de setor ou saírem da empresa, ou desconfiarem que alguém descobriu uma das senhas, elas são alteradas imediatamente.

4.12 Demais considerações

Outras medidas já tomadas antes, mas que após a criação de todos estes procedimentos foi passada para o papel, foram as configurações de usuários, algumas medidas como senhas com no mínimo 6 dígitos, expiração de senhas a

cada 2 meses, a ser trancada após ser errada 3 vezes, não poder alterar uma senha por ela mesma.

Também foram marcadas as opções para gerar log de acessos, para se ter um histórico do que e quando cada um acessou.

Outra medida importante, decidida pela gerência do setor, foi a remoção de todos os drivers de disquetes das estações de trabalho, eliminando assim, a entrada de vírus por disquetes e a saída de arquivos da empresa via disquetes.

Além de todas estas práticas a empresa contratou suporte em segurança de uma empresa especializada na área. Qualquer dúvida sobre segurança é consultada antes esta empresa. Também foram fechados alguns contratos de suporte com empresas especializadas em sistemas utilizadas na empresa, como suporte em Lotus Notes e suporte em Sistemas Microsoft. Pois é complicado manter os funcionários atualizados de tudo, se faz o possível, mas nem sempre se consegue acompanhar como deveria, até por que os funcionários estão sempre sobrecarregados de trabalho. Enquanto que estas empresas vivem para isso, elas têm obrigação de especializarem para resolver as dúvidas dos clientes.

Foi criada também uma VPN para troca de arquivos e mensagens com a matriz e demais filiais da empresa, entre outras medidas de segurança física, mas como a área da AUTORA era direcionada a administração da rede, de

correio eletrônico, auditoria, desenvolvimento em Lotus Domino, controle de licenças, políticas de segurança, plano de contingência, ela não participou das decisões e implantações destas últimas medidas.

O processo todo descrito neste trabalho começou em meados de 1999 e foi até a agosto de 2001.

4.13 Resultados obtidos

Muitos resultados foram notados pela equipe, logo após algumas práticas começarem a serem implantadas. A equipe sabe que existe uma política e está comprometida em segui-la. Através da Política de backup e do Plano de Contingência a equipe se sente segura, pois em caso de algum sinistro, terá como disponibilizar o sistema novamente e sabe como fazê-lo.

Em caso de dúvidas, os técnicos possuem suporte dos seus softwares para receber atendimento. Melhorou o ambiente de trabalho, propiciou espaço para gerar novas idéias nas reuniões semanais. Durante as trocas de experiências, sempre surgem idéias para melhorar ainda mais o ambiente de trabalho. Todas as idéias são ouvidas e aquelas possíveis de serem implantadas, a equipe se une para colocar em prática.

A empresa sempre sofreu auditoria, tanto de setores de auditoria da matriz, como de empresa externa Price. Desde que estas medidas foram implantas, os relatórios finais dessas auditorias vem trazendo menos não-conformidades a cada auditoria.

Como não é possível divulgar o conteúdo destes relatórios, por conterem informações sigilosas sobre a segurança da empresa, foi anexado neste trabalho uma carta do chefe de suporte da empresa, responsável por receber o relatório final destas auditorias, onde ele declara as melhorias obtidas após a implantação das medidas citadas neste trabalho, conforme Anexo VIII.

Na 7ª Pesquisa Nacional sobre Segurança da Informação [PNS 01], realizada pela Módulo em julho de 2001, um dos gráficos mostra as medidas de segurança mais utilizadas pelas empresas, conforme mostra a figura 4.1.

A maioria destas medidas são propostas neste trabalho, com a intenção de minimizar a ocorrência da maioria dos principais problemas mostrados no capítulo 2.

		2000 %	2001 %
1º.	Firewall	89	83
2º.	Prevenção contra vírus	93	78
3º.	Proxy Server	69	71
4º.	Segurança na sala dos servidores	72	62
5º.	Sistema de backup	91	61
6º.	Software de controle de acesso	65	61
7º.	Monitoração de log	58	56
8º.	Cofre anti-incêndio	62	43
9º.	Fragmentadoras de papel	60	41
10º.	Plano de contingência	58	41
11º.	Capacitação e treinamento	52	40
12º.	Termo de responsabilidade	49	40
13º.	Contratação de empresas especializadas	35	40
14º.	Prevenção contra pirataria	54	39
15º.	Sistema de detecção de intrusos	-	37
16º.	Sistema de criptografia	48	35
17º.	Procedimentos formalizados	34	33

Figura 4.1: Medidas utilizadas [PNS 01]

CONCLUSÃO

Através deste estudo, foi possível identificar problemas, alguns graves, outros nem tanto, que ocorrem por falta de segurança básica nas empresas e que podem acontecer em qualquer empresa, independente do porte ou do tipo de negócio.

Além disso, as medidas propostas neste trabalho são simples de serem implantadas por qualquer empresa, desde que, exista comprometimento dos usuários e técnicos e apoio da diretoria da empresa.

De acordo com o estudo realizado, foi possível mostrar que a preocupação com a segurança deve ter um lugar de destaque, não apenas para as pessoas que trabalham diretamente na área de informática, como técnicos, analistas, programadores, como também para as pessoas que, de alguma forma, utilizam a informática como ferramenta para facilitar seus trabalhos.

Enfim, que este trabalho seja um início para que outros pesquisadores possam explanar mais a respeito da segurança da informação, pois se trata de um

assunto que deve ser atualizado sempre, pois novos problemas e técnicas de soluções surgem a cada dia.

REFERÊNCIAS BIBLIOGRÁFICAS

[BER 97] BERNSTEIN, BHIMANI, SCHULTZ, SIEGEL. ***Segurança na Internet****.* Rio de Janeiro, Ed. Campus, 1997.

[CAR 00] CARISSINI, Leonardo. ***Proteção no acesso à Internet: apenas Firewall não é garantia de segurança****.* Artigo, Modulo.
Disponível em: http://www.modulo.com.br
Consultado em: Dezembro/2000

[CER 01]COMPUTER EMERGENCY RESPONSE TEAM(CERT/CC).
Estatísticas sobre incidentes de seguranças.
Disponível em: http://www.cert.org
Consultado em: Outubro/2001

[CSI 01]COMPUTER SECURITY INSTITUTE
Disponível em: http://www.gocsi.com
Consultado em: Outubro/2001

[FAV 00]FAVERO, Alberto. ***A necessecidade de Auditoria Permanente de Segurança.*** Palestre no Security Forum 2000, São Paulo, março 2000

[FON 00] FONTES, Edison, ***Vivendo segurança da informação****.* São Paulo, Ed. Sicurezza, 2000.

[FON 99] FONTES, Edison, ***Segurança da informação não é uma atitude, são muitas****.* Artigo, Jornal da Segurança, Ano 6, Número 64, dez/1999.

[GCC 01]Global Continuity.com
Disponível em: http://www.globalcontinuity.com
Consultado em: Outubro/2001

[GOM 01] GOMES, Olavo José Anchieschi. ***A Criminalidade Cibernética e suas Conseqüencias Legais.*** Reportagem de capa, Security Magazine, Ano II, Número 8, Janeiro/2001.

[INS 01]INTERNET/NETWORK SECURITY
Disponível em: http://netsecurity.about.com
Consultado em: Outubro/2001

[MSK 99] MCCLURE, SCAMBRAY, KURTZ. ***Hacking Exposed: Network Security Secrets and Solutions.*** São Paulo, Ed. McGraw-Hill, 1999.

[NET 01]NetSec, Internet Security. ***Técnicas de Ataque utilizadas na "Simulação de Ataque Hacker"***
Disponível em: http://www.netsec.com.br/servicos/sah_tecnicas
Consultado em: Novembro/2001

[PAN 00] PANETTA, Nestor. ***Criptografia.*** Reportagem de capa, Security Magazine, Ano I, Número 6, Setembro/2000.

[PAU 00] PAULA, Anchises. ***Implementando o Firewall.*** Reportagem de capa, Security Magazine, Ano I, Número 3, Março/2000.

[PWC 01]PRICEWATERHOUSECOOPERS
Disponível em: http://www.pwcglobal.com
Consultado em: Outubro/2001

[PNS 01]PESQUISA MÓDULO. ***7ª Pesquisa Nacional sobre Segurança da Informação.***
Disponível em: http://www.modulo.com.br
Consultado em: Julho/2001

[RAB 00] RABELLO, Luis. ***Proteja-se! Você vale o que transporta.***
Disponível em: http://www.modulo.com.br
Consultado em: Julho/2000

[RID 00]RIDOLFI, Lorenzo. ***Como é Possível Medir e Acompanhar o Cumprimento da Política de Segurança Definida para a sua Empresa?***
Palestra no Security Forum 2000, São Paulo, março 2000

[SAL 00] SALDANHA, Fernando. ***O Sabor do Plano de Contigência.*** Artigo, Security Magazine, Ano I, Número 6, ago/set/2000.

[SEC 01]INFORMATIVO MÓDULO. ***Modulo e-Security News - n° 188***
Disponível em: http://www.modulo.com.br
Consultado em: Abril/2001

[SEC 02]INFORMATIVO MÓDULO. ***Modulo e-Security News - n° 195***
Disponível em: http://www.modulo.com.br
Consultado em: Junho/2001

[SEC 03]SITE MÓDULO. ***Modulo e-Security News***
Disponível em: http://www.modulo.com.br
Consultado em: Maio/2001

[SEM 01]SEMÔLA, Marcos. ***No Limite da Insegurança***
Disponível em: http://www.modulo.com.br
Consultado em: Março/2000

[SPO 01] SPOHN, CAMPELLO, SERAFIM. ***Segurança em Redes TCP/IP***
UNISINOS. São Leopoldo. Junho/2001

[THO 00]THOMÉ, Andrea. ***British Standart 7799 – Um Guia para as Políticas de Segurança.*** Palestra no Security Forum 2000, São Paulo, março 2000

[VIC 00]VICECONTI, Carlos. ***Porque e Como proteger a empresa Dela mesma: Os Riscos, Necessidades e Soluçõespara Implementar a Segurança Interna nas Empresas.***
Palestra no Security Forum 2000, São Paulo, março 2000

[VUL 03]UNICAMP. ***Vulnerabilidades de softwares***
Disponível em: http://www.security.unicamp.br/docs/bugs/index.html
Consultado em: Setembro/2001

[XIM 00] XIMENES, Fernando Barcelos, *Segurança Máxima.* Rio de Janeiro, Ed. Campus, 2000.

ANEXOS

Anexo I - Formulário de Pedido de Acesso

Pedido de Acesso

Criado em **16/11/2001 10:46** por **Adriana Sette**

Para **Maria da Silva**
Digitar o nome completo do usuário.
Nº Funcional: **321654** Departamento: **Compras** Ramal: **5555**

Selecione o tipo de acesso: ☒ ERP ☒ Rede ☒ Notes

◉ Aprovado ○ Reprovado
por **Adriana Sette** em 16/11/2001 11:15

ERP **Aberto**
☒ Consulta
☒ Alteração
☒ Criação
Módulos/Telas: Requisição de Compras
Obs.:

Rede **Fechado**
◉ Criação
○ Acessos
☐ Consulta
☐ Alteração
Diretório onde será criada a pasta pessoal : X:\Compras
Diretórios para o acesso solicitado:
Grupos que o usuário deverá pertencer: Compras
Obs.:

Notes **Em Execução**
Motivo: Facilitar a Comunicação para execução das suas tarefas
Incluir nos grupos: Compras
Necessita de endereço externo ? ◉ **Sim** ○ **Não**
Marque **Sim** se o usuário deverá ter acesso a enviar e receber mails externos. Se o usuário irá usar apenas para comunicações internas a opção é **Não**.
Justifique: Comunicação com fornecedores
Obs.:

Anexo II – Políticas de Segurança

Parte do texto das Políticas de Segurança de empresa onde a AUTORA trabalhou:

(...) O Departamento de Tecnologia da Informação (DTI), responsável pelo desenvolvimento, manutenção e suporte do Hardware e Software que servem de apoio para as operações diárias da empresa X, está divulgando a partir de Fevereiro de 2000, a **POLÍTICA DE UTILIZAÇÃO DOS RECURSOS DE SISTEMAS.**
Este trabalho foi desenvolvido seguindo orientações e recomendações das áreas de Auditoria e Tecnologia da Informação da matriz da empresa. Portanto, solicitamos seja feita uma leitura com muita atenção do documento que está sendo distribuído. Ele contém instruções para todos os funcionários.
Cada funcionário deverá tomar ciência das mesmas e assinar um termo de compromisso de que respeitará esta Política de Utilização dos Recursos de Sistemas. Isto significa que é responsabilidade de cada um, tomar as medidas apropriadas para proteger as informações e os sistemas computacionais.
Este documento fornece linhas de conduta que todos os departamentos devem seguir. Ele também informa sobre as penalidades que serão impostas pelo não cumprimento das determinações. Elas foram feitas para proteger a companhia e você. Você deve cumprir com estas instruções. O seu descumprimento resultará em ações disciplinares e qualquer falha de conduta seria em relação aos procedimentos constantes nesta política poderá ocasionar a demissão e, dependendo da gravidade, levar a um processo criminal.
Os procedimentos constantes na política têm, como principal objetivo, respeitar os ativos de nossa companhia, dentro dos padrões de legalidade e ética, buscando maximizar a performance de nossas operações.
Cada departamento possui um facilitador que é responsável pelas questões de segurança e utilização dos sistemas computacionais de cada área. É sua responsabilidade questionar o gerente, o facilitador ou o gerente do DTI sobre qualquer aspecto referente a estas linhas de ação.
É muito importante que você entenda como a informação contida neste documento se aplica a você e a seu trabalho.

AMBIENTE DE REDE

Descrição: consiste no meio de tráfego, armazenamento e execução de aplicações e sistemas dentro dos negócios da EMPRESA. Este meio é protegido por níveis de segurança e administrado pelo Departamento de Tecnologia da Informação (DTI).

Composição: o Ambiente de rede é composto por servidores de dados, meios físicos de tráfego de dados, estações e ferramentas para a execução do mesmo. (...)

Toda e qualquer alteração na configuração do hardware e software do ambiente de rede (inclui computadores e seus acessórios) deve ser precedida de autorização pelo DTI.

Havendo utilização irracional dos drives, constatada por auditoria efetuada pelo DTI, este notificará o usuário, orientando-o com relação a forma correta de utilização. O usuário estará obrigado a seguir estritamente as orientações do DTI, sob pena de advertência. Reincidente ou contumaz, poderá o usuário sofrer rescisão contratual passível por justa causa.

Acesso ao ambiente de rede: o acesso à rede é dado pelo DTI através da inclusão do funcionário. A solicitação do cadastro é realizada pelo facilitador, com a aprovação do gerente direto do funcionário que receberá a conta. Fica também, sobre o mesmo, a responsabilidade de comunicar ao DTI, quanto ao desligamento do funcionário do seu grupo e a Gerência do R.H. quanto ao desligamento da empresa. O acesso é pessoal e intransferível, onde o usuário é responsável pelo direitos que lhe são conferidos e pelos atos cometidos por ações de “empréstimos” de acesso. O "empréstimo" de senha é mau procedimento, o que ensejará, por parte da Empresa a advertência escrita. A reincidência ou contumácia poderá ensejar a rescisão contratual passível por justa causa. Eventual dano constatado, material ou moral, à EMPRESA ou a terceiros, é passível de indenização pelo empregado que empresta senha.

O acesso poderá ser cancelado quando:

a) ultrapassar o prazo de validade da senha

b) o usuário fornecê-la incorretamente por até três vezes

c) ocorrer a rescisão de contrato do usuário com a empresa

d) houver má-fé na utilização dos recursos do ambiente de rede da empresa através de solicitação ou monitoramento pelo DTI passível das penalidades descritas no parágrafo anterior.

- Consulte seu gerente e CERTIFIQUE-SE de que entende claramente quais são os sistemas computacionais que você tem permissão para usar, o que você está capacitado a fazer com as informações (somente leitura, modificações, etc.) e qual a ação disciplinar que será tomada se você quebrar as regras.
- NÃO USE computador sem permissão.
- NÃO TENTE acessar informação nos sistemas computacionais sem que esteja autorizado.
- NÃO INSTALE programas pessoais ou não autorizados em nenhum computador.
- NÃO USE nenhum computado para uso pessoal, sem autorização de seu gerente.

A empresa se reserva o direito de examinar o conteúdo de todos os computadores, arquivos, conjunto de dados, discos, fitas e todo o tráfego de comunicação sem prévio aviso.

Senha: é composta por no mínimo 6 caracteres podendo ser numérica, alfabética ou uma combinação de ambos.

A sua senha e a identificação do usuário funcionam como chave para acesso aos computadores e seus sistemas. Deixar qualquer outra pessoa conhecer sua senha é como assinar um cheque em branco. Tudo aquilo que eles fizerem será registrado com o seu nome. Se uma fraude ou um delito for cometido, como você se defenderá?

- É SUA RESPONSABILIDADE manter sua senha secreta.
- NÃO compartilhe sua senha.
- Mude sua senha REGULARMENTE.
- NÃO USE a senha de outra pessoa
- NÃO escolha senhas de fácil adivinhação, como nome de familiares, datas, placas de carro ou número de crachá, números seqüenciais, como por exemplo: 123456, etc.
- SEMPRE se desconecte da rede (log off) antes de sair da frente de seu computador, para que seja necessária a re-introdução da senha.
- Se você desconfiar que alguém sabe a sua senha, mude-a e avise imediatamente seu gerente e o gerente do DTI.
- NÃO inclua a senha em arquivos de lote, *scripts*, procedimentos ou arquivo de dados.

Proteção contra perdas:

e) Os dados contidos em nossos servidores possuem um processo de salvaguarda (*backup*).

f) Este processo NÃO INCLUI os discos fixos locais de cada computador, sendo assim, É DE RESPONSABILIDADE DO USUÁRIO fazer com que seus dados sejam colocados nos diretórios da rede para que estejam garantidos.

g) Quando ocorrer a recuperação de sua cópia de *backup*, todo o trabalho realizado desde a execução do mesmo terá que ser repetido. Certifique-se de manter todos os documentos necessários para isto.

h) Verifique se existe um computador alternativo que você possa usar caso o seu falhe.

Confidencialidade: As regras que regem o nível de acesso aos dados eletrônicos não são diferentes daquelas usadas para os documentos físicos. Seu gerente estará consciente da classificação de todos os dados de sua área existentes em meio eletrônico. Ele fornecerá as diretrizes para garantir que o acesso esteja controlado de acordo.

- CERTIFIQUE-SE de ter uma clara compreensão pelo seu gerente de qual informação você tem permissão para acessar, a quem esta informação pode ser mostrada ou fornecida e que ação disciplinar será tomada caso você ignore a regra.
- NUNCA deixe o computador com informações na tela sem sua presença.

Retenção de registros: Arquivos obsoletos são um desperdício. Algum dia, por engano, eles podem ser confundidos com a informação atual.

- REMOVA arquivos desnecessários REGULARMENTE.
- Se você necessitar manter ARQUIVOS ANTIGOS, SEPARE-OS das informações atuais para evitar qualquer possibilidade de confusão e verifique a possibilidade de guardá-los em outra mídia fora da rede.
- USE O MESMO PROCEDIMENTO EMPREGADO PARA DOCUMENTOS EM PAPEL.

- **Espírito de equipe:** Tornar-se o especialista em computadores do departamento é muito bom até que você fique doente ou saia de férias e ninguém mais consiga lidar com os sistemas. É essencial que alguém mais possa substituí-lo ou que lhe dê a cobertura. Sendo assim:

- TREINE OUTRAS PESSOAS dentro de seu departamento para que alguém possa substituí-lo
- ESCREVA seus procedimentos (mas não sua senha) e mantenha-os atualizados.

PROTEÇÃO CONTRA VÍRUS

O vírus é um programa de computador que se esconde dentro de outros programas e pode causar muitos estragos. Ele pode se espalhar sempre que uma informação for passada de um computador para outro. O vírus pode "hibernar" por um determinado período de tempo antes de provocar toda a destruição. Então:

- NÃO use um disquete, a menos que tenha sido guardado chaveado ou o tenha recebido em envelope fechado de uma fonte aprovada por seu gerente. Se precisar usar disquete, verifique antes se o mesmo não contém vírus. Se necessitar, busque ajuda com seu facilitador ou gerente.
- NUNCA use disquetes sem dono, sem identificação, ou, também, como aqueles recebidos via *e-mail* ou distribuídos em revistas.
- Se o seu computador estiver conectado a uma rede pública, NUNCA use a rede da EMPRESA para receber um programa.
- Se o seu computador apresentar um comportamento estranho como: cartas que voam da tela, mensagens obscenas aparecendo, arquivos desaparecendo, então pode ser que haja um vírus. Você DEVE reportar isto, imediatamente, para seu gerente e para o gerente do DTI.
- Certifique-se que o software anti-vírus esteja ativo em todo computador que você use e que está agindo sobre todos os arquivos recebidos.

MODEMS

Os *modems* são um risco à segurança, pois podem prover acesso externo aos dados da companhia. Todo uso de *modems* deve ser autorizado pelo gerente do DTI. Em alguns casos, um procedimento operacional de segurança deverá ser preparado.
Exceto autorizado:

- Não conecte um *modem* a um computador que esteja conectado à rede da EMPRESA.
- Nunca use um modem para comunicar dados confidenciais. Isto só é permitido através do uso de *modems* especiais.
- Nunca deixe um *modem* conectado a um computador e em funcionamento durante toda a noite.

INTERNET

Descrição: Ação de utilização do recurso de acesso a rede mundial de informações e serviços (internet) **viabilizado através de um servidor de acesso da EMPRESA.**
Composição: caracteriza-se por um navegador (browser), instalado na estação do usuário, devidamente configurado para acesso através de um servidor executado sob o ambiente de rede
Solicitação de acesso: o acesso à internet é dado através da configuração do navegador na estação e no próprio login de acesso do usuário. **A solicitação do acesso deve ser feita pelo facilitador com a provação do gerente através dos Pedidos de Acessos.**
Acesso à Internet: este recurso é disponibilizado pela EMPRESA, sem limite de horas, tendo em vista os benefícios oferecidos em termos de intercâmbio, pesquisas, estudos e acessos à distância. Alguns fatores configuram a necessidade do acompanhamento da sua correta utilização. São eles:

i) o acesso à internet resulta em uma porta de entrada na rede, expondo-a a ataques de vírus e entidades com fins de manipulação ilícita das propriedades intelectuais de nossa empresa.

j) A utilização da internet acarreta em relativa perda de performance no tráfego da rede para o grupo do usuário que a utiliza.

k) Apesar da diversificação de sites da Internet, o funcionário deverá restringir-se ao acesso de informações relativas a atividades profissionais ligadas ao negócio da empresa.

l) Toda a carga de programas da internet (download) ou de clientes, fornecedores, vendedores ou de outro meio externo (via FTP ou outro protocolo) deve obter aprovação do DTI.

Por estes motivos, a empresa se reserva o direito de monitorar o uso da internet nas estações que compõe a sua rede, através de ferramentas de análise. O monitoramento do uso da Internet é facultado à Empresa, que detém os direitos sobre os meios informáticos com exclusividade. As irregularidades serão punidas com advertência escrita ou com rescisão contratual, passível por justa causa, sem prejuízo das indenizações devidas, no caso de dano material ou moral, à empresa ou a terceiros que esta tenha que indenizar.

O acesso à internet é configurado no perfil de rede do usuário requisitante, sendo este acesso pessoal e intransferível, onde o usuário é responsável por este recurso e pelos atos cometidos por ações de “empréstimos” de acesso. O "empréstimo" de senha é mau procedimento, o que ensejará, por parte da Empresa, na advertência escrita. A reincidência ou contumácia poderá ensejar a rescisão contratual, passível por justa causa. Eventual dano constatado, material ou moral, à empresa ou a terceiros, é passível de indenização pelo empregado que empresta senha.

A transferência de documentos confidenciais, via Internet, é terminantemente proibida. Exemplos de documentos confidenciais, mas não limitados a estes, são: contratos, planos

de negócios, acordos de negócios, desenhos de controle dimensional, planilhas de custos, dados contábeis e dados de folhas de pagamento e salários. A publicação de informações na Internet deve ser previamente aprovada pela Alta gerência.

LOTUS NOTES

Descrição: o Lotus Notes caracteriza-se por uma ferramenta de intercâmbio de informações dentro da rede Global de nossa empresa com alto potencial de automatização de tarefas documentais.
Composição: software cliente instalado nas estações dos usuário, sendo executado sob ambiente operacional (Windows95, Windows Workstation...)
Solicitação de acesso: o acesso ao sistema de correio eletrônico, Lotus Notes, é dado através do formulário eletrônico de solicitação de pedido de acesso procedido pelo gerente direto do usuário a receber a conta..
Utilização do Lotus Notes: a utilização desta ferramenta de distribuição de documentos condiciona os seus usuários a manterem as suas caixas postais organizadas, principalmente quanto ao descarte de mensagens que não serão mais úteis. Conseqüentemente, a EMPRESA adotou as seguintes normas sobre o uso do E-mail por seus empregados:

m) Sistema de E-mail é de propriedade da empresa é destina-se unicamente a ajudar os empregados na condução dos negócios da companhia. A EMPRESA tem o direito de entrar no sistema de E-mail e revisar, copiar e excluir qualquer mensagem, bem como revelar as mensagens a outros. Não presuma que as mensagens sejam confidenciais em função do uso de uma senha, uma vez que essas medidas servem para proteção da EMPRESA, e não do empregado que usa o sistema.

n) Os usuários do E-mail devem, portanto, manter suas mensagens em caráter profissional e evitar usar o sistema para bate-papos e mensagens pessoais. O E-mail não deve ser profano, vulgar, difamatório ou embaraçoso em sua natureza e conteúdo, sendo passível das penas do parágrafo “E” desta norma. NÃO TRATE informações sobre pessoas (significa qualquer informação que inclua uma opinião ou um fato sobre determinada pessoa), a menos que tenham sido aprovadas pelo Departamento de Recursos Humanos. Você deve informar ao gerente de Recursos Humanos ou ao gerente do DTI sobre qualquer informação que necessite processar referente a pessoas. Existem leis que impõem obrigações a qualquer um que tratar de informações sobre pessoas. Penas de prisão ou multas podem ser impostas sob determinadas circunstâncias.

o) O pessoal da EMPRESA deve reconhecer que as informações confidenciais não devem ser enviadas via E-mail para fora da companhia ou até mesmo para empregados dentro da companhia, a menos que o recebedor da mensagem esteja autorizado a receber tal informação. Todos devemos reconhecer que as informações transmitidas via E-mail podem conter segredos comerciais ou informações confidenciais, e que devem ser tomadas as providências cabíveis para proteger a segurança de tais informações. Os profissionais de computação da EMPRESA podem fornecer orientações sobre as precauções de segurança.

p) É proibido trafegar com “correntes”, multiplicando o número de usuários destinatários. Este procedimento resulta em sobrecarga no sistema, afetando as caixas postais dos destinatários com mensagens sem cunho profissional e o próprio banco notes com a multiplicação destas mensagens, sendo passível do cancelamento da conta do usuário que faz uso desta ação.

q) "Empréstimo" de senha é mau procedimento, o que ensejará, por parte da Empresa na advertência escrita. A reincidência ou contumácia poderá ensejar a rescisão contratual, passível por justa causa. Eventual dano constatado, material ou moral, à EMPRESA ou a terceiros, é passível de indenização pelo empregado que empresta senha.

UTILIZAÇÃO DE SOFTWARES

Descrição: constitui-se no ato de manipulação de software (ambientes operacionais, ambientes de rede, aplicativos, ferramentas, etc) instalados ou não na estação do usuário.
Composição: caracteriza-se pelo meio de transporte do software (magnético, óptico ou download), manuais e licença.
Solicitação de software: a solicitação de aquisição de software é efetuada através de formulário preenchido e entregue ao DTI que efetuará a análise e iniciará o processo de liberação do mesmo (solicitação de recurso via Lotus Notes).
Instalação de software: a instalação de software, seja na estação do usuário ou no ambiente de rede, somente poderá ser procedido pelo DTI, salvo com autorização prévia. Toda e qualquer instalação, quando autorizada pela Gerência do DTI, deve ser imediatamente reportada pelo usuário.
PIRATARIA: é a cópia não autorizada de programas ou outros materiais com direitos exclusivos de cópia.

- NÃO faça cópias não autorizadas de programas.
- SOMENTE use programas APROVADOS e comprados através de canais oficiais. Questione seu gerente se tiver dúvidas.

Verifique seu computador. Se você encontrar qualquer programa que não seja aprovado, notifique seu gerente E o gerente do DTI.

O ato de instalação, sem autorização, será caracterizado como deturpação dos direitos autorais do autor do software, ato este passível de ações legais pelo próprio autor e repudiado pelos padrões de conduta da EMPRESA. A configuração deste ato sujeitará o infrator à advertência escrita ou rescisão contratual passível por justa causa, independentemente das indenizações devidas à EMPRESA ou a terceiros. Em qualquer das irregularidades descritas, constatado o dolo ou má-fé do usuário, a Empresa procederá a rescisão contratual, passível por justa causa, em caráter imediato.

(…)

Anexo III – Parte do Procedimento de Auditoria

A auditoria visa verificar se as ferramentas de sistemas estão sendo utilizadas de acordo com o estabelecido na Política de Utilização de Recursos de Sistemas da empresa.

Esse documento visa esclarecer o procedimento de auditoria utilizado para auditagem de arquivos. Almejando arquivos que por seu conteúdo possuam dados, imagens, informações que não façam parte do negócio da empresa ou que não façam parte da atribuição de quem tem acesso ao mesmo.

As informações contidas neste documento são extremamente confidenciais e dizem respeito somente ao pessoal do GRUPO DE SUPORTE do DTI (Sistemas) da empresa.

Varredura de mensagens no servidor NOTES

Aqui são analisadas mensagens e pastas do usuário dentro da caixa de correio, verificando se o seu uso está de acordo com a Política de Utilização de Recursos de Sistemas da empresa.

O critério para escolha de usuários para essa auditoria é também o software que realiza o sorteio ou a incidência de ser encontrado um arquivo incondizente com o negócio da empresa na varredura de arquivos.

É também verificado se o usuário em questão tem pedido de acesso liberado para receber mensagem externa, e é testado se o usuário recebe mensagem externa.

Varredura de páginas acessadas na INTERNET

Aqui um relatório do "proxy server" permite visualizar as páginas acessadas, e a partir daí identifica-se os nomes suspeitos e entra-se na página para conferir se o conteúdo é condizente ou não, e quem estava acessando, quando e onde.

É conferido também se o usuário em questão tem um pedido de acesso liberado pela gerência para fazer uso dessa ferramenta.

Periodicidade da auditoria

As auditorias são mensais, ou a critério da gerência.

Anexo IV – Exemplo de Relatório de Auditoria

Porto Alegre, 07 de maio de 2001.

Referente auditoria realizada no mês de abril.

Logins sorteados: asilva, fmachado, dpereira, cnunes, maraujo.

Não conformidades encontradas:

Na varredura de rede e nos micros locais não foram encontradas não conformidades nestes logins. Na varredura de ERP foi identificado que o login fmachado foi transferido de setor e continuava com os acessos antigos, o que foi alterado imediatamente. Estes logins não possuem acesso a internet, por isso, não foi gerado log de acessos à internet deles. Na varredura do Correio eletrônico foram encontrados alguns mails recebidos de correntes na caixa postal do login maraujo, mas não foram encontrados indícios de que o usuário tenha repassado estes mails para outras pessoas.

Responsável pela auditoria: Adriana Sette

Anexo V – Procedimentos da Backup

Este documento tem por objetivo explicar o processo de back-up da empresa, incluindo explanações sobre o uso do cofre: localização, especificações; e o processo de gerenciamento das fitas via software.

Métodos de BACKUP

A cópia de salvaguarda ocorre na empresa diariamente, utilizando dois métodos:

- O método FULL

  Consiste na cópia de tudo que estiver no servidor alvo, independentemente da data de modificação, todos arquivos são copiados;

- O método DIFERENCIAL ou CUMULATIVO

  Consiste na cópia somente dos arquivos que sofreram modificação desde o último backup FULL do mesmo POOL; (...)

  Por tratar-se de um documento com informações sobre os servidores, localições de fitas e demais itens particulares da empresa, este procedimento não poderá ser mostrado na íntegra.

Anexo VI – Rotinas de Backup

Exemplo de Rotinas de Backup - visão de servidores

Servidor FLORIPA, servidor de arquivos

O que está sendo copiado?	Qual a periodicidade das cópias?	Tipo de Backup	Por quanto tempo é preservada a cópia?	Média de espaço necessário	Nome do arquivo de Job no arcserve
E:\APLIC	24 em 24h	Incremental	7d	1.2Gb	Diario.asx
E:\SOFTDADO	24 em 24h		7d	2.8Gb	Diario.asx
E:\USUARIOS	24 em 24h		7d	23.5Gb	Diario.asx
E:\APLIC	7 em 7d	Full	1m	1.2Gb	Semanal.asx
E:\SOFTDADO	7 em 7d		1m	2.8Gb	Semanal.asx
E:\USUARIOS	7 em 7d		1m	23.5Gb	Semanal.asx
E:\APLIC	1 em 1m	Full desde a último semestre	12m	1.2Gb	Mensal.asx
E:\LOGs	1 em 1m		12m	80Mb	Mensal.asx
E:\SOFTDADO	1 em 1m		12m	2.8Gb	Mensal.asx
E:\USUARIOS	1 em 1m		12m	23.5Gb	Mensal.asx
Registry Files	1 em 1m		12m	15Mb	Mensal.asx
E:\APLIC	6 em 6m	Full	5 anos	1.2Gb	Semestral.asx
E:\LOGs	6 em 6m		5 anos	80Mb	Semestral.asx
E:\SOFTDADO	6 em 6m		5 anos	2.8Gb	Semestral.asx
E:\USUARIOS	6 em 6m		5 anos	23.5Gb	Semestral.asx
Registry Files	6 em 6m		5 anos	15Mb	Semestral.asx

Totais :
Diário : 27.5Gb

Anexo VII – Sites sobre segurança

http://www.security.unicamp.br/docs/bugs/index.html - vulnerabilidades de segurança.

http://www.gus.com.br/ - artigos sobre segurança fisica, lógica e de informação.

http://www.securenet.com.br/index.php - segurança da informação.

http://researchindex.com - biblioteca digital da literatura científica.

http://www.cert.org.br - vulnerabilidades, estatísticas, ferramentas.

http://www.pwcglobal.com - segurança da informação em geral

http://www.isaca.org - segurança da informação em geral

http://www.gocsi.com - segurança da informação em geral

http://netsecurity.about.com - segurança da informação

http://www.globalcontinuity.com - continuidade de negócios

http://www.auscert.org.au/Information/Auscert_info/Papers/Security_Domains.html - firewalls

http://www.sans.org/newlook/resources/glossary.htm - firewalls

Anexo VIII – Carta da empresa

GKN Automotive

ATH

GKN do Brasil Ltda.
Av. Joaquim Silveira, 557, Porto Alegre, RS, CEP: 91.060-320, Brazil
Tel: (55) (51) 3349 9500 Fax: (55) (51) 3349 9300

À ULBRA – Universidade Luterana do Brasil

Porto Alegre, 23 de Novembro de 2001

Declaro para os devidos fins que a Adriana Aparecida Sette teve grande participação nos processos internos de segurança implantados nesta empresa, principalmente no que diz respeito aos controles de acessos, instalação e configuração de regras de segurança no firewall e auditorias de utilização de sistemas. Este trabalho foi de fundamental importância na implantação dos nossos procedimentos e políticas internas de segurança.

Atenciosamente,

Giovani Sartori
Chefe de TI – Suporte Técnico
GKN do Brasil Ltda.