Convergência Segurança Física e Lógica

Hoje em dia segurança envolve desde os prédios e equipamentos como também proteção de redes, privacidade, etc.

Até hoje a maioria das organizações trabalham com segurança física e lógica, completamente separadas, inclusive administradas por departamentos separados.

Facilidades de acesso comprometem a segurança de uma empresa. Tendo acesso físico se pode roubar um PC, roubar informações além de comprometer a sua rede, tanto fisicamente como logicamente.

Abaixo algumas matérias relacionadas ao assunto:

• A Petrobras confirmou nesta quinta-feira que dados sigilosos sobre pesquisas sísmicas, que podem incluir a descoberta de petróleo e gás, foram furtados de um contêiner da empresa. (Folha, 2009).

• Escola tem todo laboratório de informática roubado Este foi o 5º assalto. Perdas devem superar os 10 mil (Ipoom,2009).

• Criminosos da computação violam regularmente sistemas de segurança e roubam milhões de dólares e dados de cartões de crédito (Terra, 2009).

Como foi visto nas matérias acima os criminosos estão utilizando tanto o meio físico quanto o meio lógico para conseguirem roubar informações das empresas, isso causa dúvidas nos analistas de segurança da informação, devo me proteger fisicamente ou logicamente.

Esse artigo tem por objetivo demonstrar que deve ser utilizada uma convergência entre os métodos físicos e lógicos para conseguir uma maior segurança dentro da empresa.

Nada adianta um datacenter repleto de firewalls e de outras tecnologias e um colaborador deixar a porta aberta para um criminoso entrar, do mesmo modo que colocar câmeras, cercas elétricas, iluminação, e não ter nenhum controle lógico.

O que é Segurança Física

É tudo que não é lógico, nossa, mas isso é óbvio demais, vamos tentar melhorar a nossa explicação, a segurança física é extremamente importante para manter a integridade, confidencialidade e disponibilidade das informações da sua empresa. Um exemplo pode ser o computador ele é algo físico. Sem a segurança física o acesso de uma pessoa não autorizada a um computador pode resultar em divulgação da informação, alteração da informação e também destruição da informação.

Alguns controles possíveis com a segurança física:

• Controles de acesso;

• Controles de intrusão;

• CFTV;

• Alarmes (incêndio, invasão do prédio, entre outros);

• Entre outros;

O Que É Segurança Lógica

É tudo o que não é físico, nossa essa piada de novo? Bom, tentaremos novamente, resumidamente segurança lógica é o modo como as informações são protegidas dentro de um sistema, por exemplo, restrição de acesso a um banco de dados com login e senha pode ser considerado segurança lógica.

Controles possíveis com segurança lógica:

- Criptografia de arquivos;
- Controle de acesso a internet;
- Entre outros;

O Que É Convergência Física E Lógica

A convergência física e lógica nada mais é do que integrar ambas, por exemplo, vamos imaginar um cenário que tenhamos câmeras espalhadas pela empresa inteira, porém apenas as câmeras são ineficientes para fins de investigação, ou seja, apenas exibi o que acontece naquele momento, mas sem gravar nada.

Uma forma de realizar uma convergência é exatamente começar a gravar os dados, ou seja, tudo que for filmado você irá armazenar em um computador com HD suficiente para isso, essa é uma forma de convergir segurança física e lógica.

Outro exemplo suponha que a empresa possui catracas físicas, onde o funcionário passa o crachá e entra, uma integração pode ser armazenar os dados da entrada e saída do funcionário, com haverá rastreabilidade dos funcionários.

Por Que Utilizar Convergência Física E Lógica

Como mostrado acima os criminosos estão utilizando todos os meios para conseguirem roubar informações das empresas, além de utilizarem os meios lógicos eles também estão utilizando o meio físico e muitas vezes roubando equipamentos e posteriormente roubando também dados lógicos.

Nessa linha que a convergência pode ajudar a melhorar a eficiência da segurança, onde se pode entregar uma credencial a um funcionário e com essa credencial ele pode acessar as áreas e sistemas que foram vínculos a ele.

Com isso pode ter um controle das áreas que o funcionário entrou que horas ele entrou, que horas saiu, permitindo assim uma rastreabilidade do mesmo, inclusive verificando onde o funcionário tentou entrar e não foi permitido devido ao seu perfil.

Outro fator da convergência é a parte de auditoria, como tudo que é feito é armazenado em informações, pode ser de extrema importância na necessidade de uma análise forense.

A convergência deve estar integrada com os processos da empresa para facilitar a administração dos mesmos, pessoas e sistemas de TI. Isto inclui:

- Política de Segurança da Informação;
- Provisionamento de usuário e ativos;
- Monitoramento e auditoria;
- Resposta a incidentes;
- Plano de continuidade de negócios;

A convergência ajuda a dificultar ataques, e ao mesmo tempo auxiliar na detecção, correção e prevenção dos mesmos.

Casos Reais

Existem sistemas especializados nessa integração entre segurança física e lógica, iremos apresentar alguns casos onde a convergência entre segurança física e lógica já é utilizado:

- Acesso físico e lógico através de cartões (crachás), onde através desse cartão é permitido o ingresso seguro à rede de Windows, bloqueio de PC, acesso remoto seguro (VPN), e e-mail seguro com assinatura digital.

• Biometria de acesso a sistemas permite as organizações mudar senhas, consolidar identidades de usuário, e assegurar informação vital da empresa. Realizar a convergência de múltiplas credenciais de usuário numa identidade individual e unificada.

• Sistema de detecção de incêndio, instalação de sensores que irão emitir alarmes tanto físico quanto lógicos, quando detectado fumaça;

Como foi dito no início do artigo muitas empresas ainda utilizam a segurança física da segurança lógica separadamente inclusive por departamentos diferentes.

Como podem ser vistos em algumas notícias mostradas no artigo os criminosos estão cada vez mais utilizando novas técnicas de ataques, e utilizam os dois meios tanto o físico quanto o lógico, nesse cenário a convergência entre a segurança física e lógica pode ajudar a mitigar alguns riscos.

A convergência melhora a eficiência e dificulta ataques, ao mesmo tempo em que pode ser uma grande ferramenta de auditoria quando da ocorrência de algum incidente.

Como A Criptografia Diferem De Um Firewall Em Termos De Segurança De Dados

Criptografia e firewalls são essenciais para os esforços de toda a organização para manter a segurança de seus ativos de dados. Estas duas peças de tecnologia efectivamente desempenham funções complementares, mesmo que um pode ser realizada por outro. A decisão nunca deve ser que as tecnologias a utilizar, mas sim como usá-los tanto de forma eficaz. Rede de Transmissão de Dados

Os dados são transmitidos através de redes na forma de pacotes, cada um dos quais tem informações de identificação embutido em seu cabeçalho. Como esses pacotes viajam em redes internas ou a Internet, eles são suscetíveis a bisbilhoteiros que " farejar" o tráfego em busca de informações úteis. Se os pacotes não são criptografadas, ou em claro, um invasor pode facilmente agarrá-los e extrair as informações que ele quer.

Cryptography

criptografia é a ciência de embaralhamento de dados com uma "chave" para uma forma indecifrável. A única pessoa que pode decifrar o pacote de dados é alguém com a chave de decodificação. Na criptografia de chave privada, a chave é a mesma em ambas as extremidades. Na criptografia de chave pública uma tecla é privado e um é público. A chave privada deve ser protegida de divulgação com qualquer método, mas com o último método a chave pública está disponível para todos.

Firewalls

Firewalls inspecionar pacotes e comparar os resultados com um conjunto de regras configuráveis. Se os critérios de pacotes cumprir uma regra de "permitir", o pacote é permitido passar. Se o pacote está na lista de " negar ", o pacote é descartado. A regra padrão mais seguro é "negar tudo ", e esta regra deve ir por último na lista de regras, que é processada de cima para baixo. Firewalls são posicionadas entre as redes, geralmente entre a rede interna de uma organização e da Internet, mas eles também podem ser posicionados entre redes internas para maior segurança.

Firewalls E Criptografia

Firewalls e criptografia são tecnologias que devem ser usados em conjunto para alcançar um perfil de segurança mais completa. Existem firewalls disponíveis que proporcionam criptografia, como uma parte da sua funcionalidade. Isso fornece uma combinação poderosa que, se um pacote criptografado atinge o firewall, eo firewall não pode decifrá-lo, o firewall descarta o pacote. A desvantagem é que a criptografia tem recursos na forma de tempo do processador. Isso exige hardware mais potente para rodar o firewall ou o seu desempenho pode sofrer, retardando o acesso à Internet e gerando reclamações de usuários. A correcta aplicação dessas tecnologias complementares podem fornecer uma segurança muito maior do que qualquer um pode fornecer sozinho.

Redes De Computadores Segurança Lógica

Firewalls

Com o avanço das redes de computadores e a possibilidade de conectar praticamente qualquer computador a outro, um grande problema surgiu aos administradores de rede, a possibilidade de um intruso acessar uma rede privada se passando por um usuário legítimo e ter acesso a informações sigilosas. (CARUSO & STEFFEN, 2006). Além disso, conforme TANEMBAUM (2003), existe ainda o problema dos vírus e worms, que podem burlar a segurança e destruir dados valiosos.

Para ajudar a manter as redes mais seguras, os Firewalls remetem à idéia de uma única passagem para os dados, onde todos são analisados antes de serem liberados e, de fato, o que acontece é exatamente isso, todo o tráfego de uma rede passa obrigatoriamente por uma estação de controle para ser analisado, caso não encontre nenhuma restrição, o Firewall libera o pacote e este segue para seu destino, caso contrário, é sumariamente descartado.

CARUSO & STEFFEN afirmam que:

“Normalmente, um Firewall é instalado no ponto de interligação de uma rede interna com a Internet. Todo o tráfego, nos dois sentidos, tem de passar por este ponto e, dessa forma, atender aos requisitos da política de segurança da instalação.”

O administrador da rede pode definir políticas específicas para a filtragem do tráfego da rede, por exemplo, pode indicar que todo o tráfego endereçado para a porta 23 seja bloqueado. Desta forma o atacante, ao enviar pacotes de fora da rede para a porta 23, será automaticamente ignorado pelo destino e ainda, o administrador poderá ser alertado sobre a tentativa.

O Firewall se divide em dois componentes: o filtro de pacotes, que faz exatamente a função exemplificada acima, inspecionando cada pacote de entrada e saída, e identificando a origem e o destino de cada um. E o gateway de aplicação que, conforme TANEMBAUM (2003), em vez de apenas examinar os pacotes brutos, o gateway toma a decisão de transmitir ou descartar a mensagem através da análise dos campos de cabeçalho, do tamanho da mensagem e até do seu conteúdo (em busca de palavras-chave). Esta última situação é bastante útil quando se deseja bloquear o acesso a conteúdos que não têm uma fonte específica, ou que são providos por um serviço onde as portas são atribuídas dinamicamente. Neste caso os pacotes passariam pelo filtro de pacotes, porém seriam bloqueados pela análise do gateway de aplicação.

Muitos Firewalls já identificam os ataques antes que consigam causar algum dano sério. Porém, um dos ataques mais comuns e que ainda é a causa de muitas indisponibilidades de serviços é o ataque de negação de serviço (DoS), onde o atacante envia milhares de pedidos de conexão ao servidor, que por sua vez responde a cada um deles, normalmente cada pedido fica retido por um tempo até que seja eliminado automaticamente pelo servidor, porém, até que isso aconteça o limite de conexões do servidor pode ser excedido, e a partir daí nenhuma conexão nova poderá ser aceita, deixando o serviço em questão indisponível para outros usuários. Para se proteger contra esse ataque o Firewall deve ser configurado para limitar a quantidade de conexões estabelecidas por cada usuário, desta forma, mesmo que o atacante utilize vários endereços de origem diferentes para conseguir várias conexões, será mais trabalhoso conseguir a negação do serviço para usuários legítimos.

Antivírus

Os vírus de computador se tornaram uma praga no mundo digital e as empresas têm gasto milhares de Dólares na busca por formas de combatê-los. Basicamente um vírus é um código malicioso que se hospeda em outro programa do computador. Segundo TANENBAUM & WOODHULL (2000), quando um programa infectado é iniciado, este começa uma varredura no disco rígido em busca de outros arquivos executáveis, quando um programa é localizado, ele é infectado anexando-se código do vírus no final do arquivo e substituindo a primeira instrução por um salto para o vírus. Desta maneira, toda vez que o usuário tenta executar um programa infectado, irá, na verdade, executar o código do vírus e estará, cada vez mais, propagando o código malicioso para outros arquivos.

Além de infectar outros programas, um vírus tem controle quase que total sobre a máquina e pode fazer muitas coisas no computador, como apagar, modificar ou bloquear arquivos do usuário, exibir mensagens na tela e, muito comumente, pode simplesmente danificar o setor de inicialização do risco rígido, impossibilitando o funcionamento do Sistema Operacional. A única alternativa para o usuário neste caso é reformatar o disco rígido e recriar o setor de inicialização.

Combater um vírus não é uma tarefa fácil (TANEMBAUM, 2003), principalmente devido ao fato de que ele pode ter embutido em seu código uma característica de mutação própria, transformando-se novamente em uma estrutura desconhecida pelo antivírus. CIDALE (1990) cita quatro formas diferentes de detecção possíveis para antivírus:

• Escaneamento de vírus conhecidos: Apesar de ser bastante antigo, este ainda é o principal método de detecção de códigos maliciosos. Assim como, na área da saúde, os médicos e infectologistas precisam conhecer parte do vírus (biológico) para desenvolver uma vacina que será aplicada em humanos, na área computacional, as empresas desenvolvedoras dos antivírus (digitais) precisam também conhecer o código malicioso para poder criar uma vacina e proteger os computadores. Uma vez que as empresas recebem o vírus, uma parte do código é separada (string) e tomada como “assinatura” ou impressão digital do vírus, que por sua vez, passa a integrar uma lista de vírus conhecidos. Esta lista é distribuída por meio de atualizações via internet para os computadores pessoais. A partir daí, sempre que o antivírus identificar em um programa a string de um vírus, este será bloqueado.

• Análise Heurística: Este processo consiste em uma análise, por parte do antivírus, em programas que estão sendo executados em busca de indícios de ações que seriam executadas comumente por vírus. Por exemplo, uma função de escrita em um arquivo executável, ou em vários arquivos executáveis de forma seqüencial, isso poderia ser um indício de que um código malicioso estaria tentando se propagar, atribuindo seu código à outro executável. Neste caso a análise Heurística do antivírus deve bloquear a ação e alertar o usuário sobre o evento. Este é um processo complexo e que nem sempre funciona como deveria, conforme CIDALE (1990), algumas funções que seriam identificadas como suspeitas podem ser totalmente normais em determinadas circunstâncias, gerando o que o próprio chama de falso positivo, que é quando um alerta de vírus é dado para um arquivo legítimo.

• Busca Algorítmica: Em comparação com o primeiro método, este processo de identificação é um pouco mais preciso, pois utiliza um conceito de busca mais complexo. Uma série de condições pode ser imposta para que o vírus seja identificado, como a extensão do arquivo, o tamanho, a string, e outros mais. Devido à sua maior complexidade, torna a pesquisa mais lenta e, por isso, acaba sendo utilizado apenas em casos onde o método de comparação de string não é eficaz.

• Checagem de Integridade: Diferentemente dos outros métodos, nesta técnica não é necessário conhecer o código do vírus anteriormente para se proteger dele. Consiste basicamente em criar um registro com os dígitos verificadores de todos os programas instalados no computador, TANENBAUM (1999) afirma que tal registro deve ser feito logo após uma formatação completa e armazenado em um local seguro no computador e criptografado. Posteriormente, quando executada uma verificação, o código verificador do programa em execução será comparado com o código armazenado no banco de dados do antivírus, caso haja alguma alteração significa que o programa foi alterado sem permissão. Tal abordagem não impede a infecção, mas permite detectar cedo a sua presença.

Como podemos perceber nenhum dos métodos disponíveis até hoje é completamente eficaz contra as pragas virtuais. O mais certo é utilizar um antivírus que esteja sempre atualizado e que possua métodos de detecção próprios eficientes como a Análise Heurística e a Checagem da Integridade, mesmo assim, deve-se sempre instalar softwares originais e de fontes confiáveis (TANEMBAUM, 1999).

Segregação De Rede

A norma NBR ISO/IEC 17799 (2005) afirma, em um dos seus controles, que um método de controlar a segurança da informação em grandes redes é dividi-la em domínios de redes lógicas diferentes. De fato, esta é uma prática comum em redes de computadores estruturadas que garante acesso restrito a certos serviços. Por exemplo, uma instituição de ensino como uma faculdade, que possui laboratórios de informática utilizados por seus alunos, não seria conveniente que eles estivessem desenvolvendo suas pesquisas na mesma rede onde se encontra o servidor de banco de dados com suas notas, faltas e vida financeira. Tais dados poderiam estar em risco. Porém, também não seria conveniente para a instituição manter uma infra- estrutura física separada para atender apenas aos laboratórios, isso sairia caro, portanto com a divisão lógica da rede é possível manter apenas uma estrutura física impondo limites logicamente.

"Tal perímetro de rede pode ser implementado instalando um gateway seguro entre as duas redes a serem interconectadas para controlar o acesso e o fluxo de informação entre os dois domínios. Convém que este gateway seja configurado para filtrar tráfico entre estes domínios e bloquear acesso não autorizado conforme a política de controle de acesso da organização".

Outra situação onde a segregação de rede se faz necessária é quando máquinas da rede precisam receber acessos externos, como é o caso de servidores Web e email, por exemplo. O fato de deixá-las no mesmo segmento de rede de outras máquinas não impediria que o serviço que elas executam funcionasse corretamente, porém, em caso de invasão todo o segmento de rede estaria em risco. O atacante poderia se utilizar de uma falha no servidor Web para ter acesso ao servidor de banco de dados da empresa e roubar informações sigilosas, além é claro, de ter controle sobre o primeiro servidor.

Neste caso, seria criada uma divisão lógica, ou uma sub-rede, chamada de DMZ (Zona Desmilitarizada). Este segmento seria protegido por um Firewall, porém, permitiria o acesso de clientes externos conforme demandam os seus serviços.

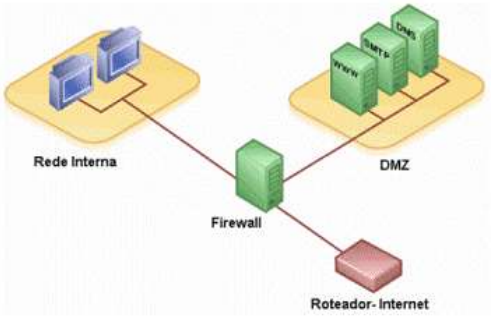

Figura 5: Segregação de rede com uma DMZ

Segundo SÊMOLA (2003), o conceito de Firewall, e que se aplica muito bem nessa situação, está ligado às paredes internas de uma construção que impedem que o fogo se propague de uma sala para outra. Caso o atacante consiga explorar uma falha em um dos serviços da DMZ, ainda não teria acesso à rede interna da corporação. A recomendação da norma NBR ISO/IEC 17799 é que "os domínios sejam definidos de acordo com uma análise de riscos e requisitos de segurança diferentes". Esta análise pode determinar a divisão da rede em vários segmentos, como sistemas publicamente acessíveis, redes internas e ativos críticos.

Controle De Acessos De Usuários

O objetivo do controle de acessos de usuário é controlar o acesso à informação. (NBR ISO/IEC 17799, 2005). CARUSO & STEFFEN (2006) afirmam que o controle de acessos leva em consideração, basicamente, duas questões que devem se respondidas antes de qualquer coisa:

- Quem irá acessar?

- Quais recursos serão acessados?

Essas duas questões irão gerar um inventário com todos os usuários e os recursos disponíveis no ambiente da empresa. Conhecendo os usuários, deve-se organizá-los em grupos por departamentos ou por funções relacionadas. A seguir, os direitos de acesso devem ser dados por pessoas autorizadas de dentro da empresa. "Convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços".

Vários usuários poderão receber as mesmas designações de acesso às informações, por isso, devem ser agrupados em entidades, e as permissões atribuídas à entidade, facilitando o gerenciamento dos privilégios.

Monitoramento

O monitoramento das atividades em um ambiente de tecnologia da informação tem como objetivo principal detectar atividades não autorizadas realizadas por usuários internos ou externos. (NBR ISO/IEC 17799, 2005). O registro das atividades deve ser feito de forma automática pelos sistemas, gerando um arquivo chamado de log. Este arquivo deve ser protegido contra falsificação e acesso não autorizado, mantendo a sua integridade e confiabilidade caso seja necessário utilizá-lo. (TANEMBAUM, 1999).

Muitos dos logs gerados trazem informações referentes não só aos acessos de usuários, mas também, informações técnicas referentes aos recursos do sistema. Essas informações podem ser úteis na resolução de problemas, pois muitos sistemas emitem alertas sobre deficiências encontradas na execução de tarefas. Desta forma registros de log geralmente contêm um grande volume de dados, tornando difícil para uma pessoa identificar eventos importantes. Por tanto, a norma NBR ISO/IEC 17799:2005 recomenda o uso de ferramentas de auditoria para a análise adequada desse material.

Alguns sistemas, como o Microsoft Windows Server 2003, por exemplo, possuem uma ferramenta de análise de logs própria, que em caso de eventos considerados relevantes envia uma mensagem para o administrador informando sobre o problema.

As atividades de todos os usuários (administradores ou operadores) devem ser registradas sejam estas realizadas em um sistema operacional ou em um software ERP. CARUSO & STEFFEN (2006) definem alguns dados como indispensáveis em um log:

- Identificação do usuário;
- Data, horário;
- Informações sobre o evento;
- Identificação do terminal utilizado.

O monitoramento pode ser feito não só através de logs, mas, também em tempo real, como é o caso dos sistemas de monitoramento de serviços. Basicamente, o administrador tem acesso às condições de operação de um ativo mesmo este estando em uso, seja um software ou hardware. E através da emissão de relatórios é possível identificar problemas, planejar melhorias ou, definir regras para uma melhor utilização da ferramenta.

Criptografia

Com a vulnerabilidade dos mecanismos de comunicação utilizados atualmente sempre existe a possibilidade de interceptação dos dados trafegados. CARUSO & STEFFEN (2006, p. 172) afirmam que “enquanto as linhas de comunicação fizerem uso de sinais elétricos para a transmissão de sinais, elas continuarão a ser vulneráveis à penetração não autorizada”. Isso se deve ai fato de que interceptar um sinal elétrico é muito simples e pode ser difícil de identificar o intruso.

Como muitas vezes é impossível garantir a confiabilidade do meio de transmissão, passou-se a utilizar uma técnica para esconder a mensagem caso esta fosse interceptada durante o trajeto. A palavra criptografia tem origem grega, significa "escrita secreta", esta técnica já é utilizada a milhares de anos. (TANEMBAUM, 1999). Consiste basicamente na substituição ou transposição de caracteres de uma mensagem.

O emissor criptografa o texto utilizando um padrão estabelecido pela chave de cifragem e envia a mensagem ininteligível. Chegando ao destino, o texto cifrado precisa ser descriptografado, realizando o processo inverso, e seguindo o mesmo padrão estabelecido pelo emissor. As chaves de cifragem dividem-se em simétricas e assimétricas.

Na criptografia simétrica a chave utilizada para cifrar uma mensagem é a mesma utilizada para voltar ao texto inteligível (CARUSO & STEFFEN, 2006). Neste caso o destinatário deve conhecer a chave utilizada pelo emissor para efetuar a troca. É um processo simples, muito utilizado pela maioria dos algoritmos, porém não muito seguro, já que se a chave for descoberta qualquer um poderá ler a mensagem cifrada. (CARUSO & STEFFEN, 2006). Um exemplo claro deste tipo de chave é a Cifra de César [21], onde cada letra da mensagem é substituída por outra do alfabeto, seguindo um número de troca de posições. Por exemplo, utilizando uma troca de quatro posições, a letra A seria substituída

pela letra E, a letra B seria F e assim por diante. Juntamente com a mensagem cifrada, o emissor deve encontrar um meio de informar ao destinatário qual a chave para descriptografar a mensagem. Nesse caso, o número de troca precisa ser informado.

Já na criptografia assimétrica, a chave usada para criptografar não pode ser usada para reverter o processo; isto só é possível com uma chave complementar. (CARUSO & STEFFEN, 2006). Um dos poucos exemplos que temos é o método de chaves públicas RSA [22]. Este método é baseado em cálculos com números primos, e se utiliza da dificuldade de fatorar tais números. Teoricamente, é perfeitamente possível quebrar a chave RSA, porém matemáticos têm tentando fatorar números extensos há pelo menos trezentos anos e o conhecimento acumulado sugere que o problema é extremamente difícil (TANEMBAUM, 1999). Na prática o algoritmo funciona da seguinte forma: primeiro um dos indivíduos (A) que participará da comunicação cria uma chave pública e envia para o outro indivíduo (B), na verdade estará enviando o algoritmo de encriptação. Depois A deve criar a chave privada que será conhecida apenas por ele próprio. B poderá enviar mensagens para A através da chave pública, porém apenas A terá a chave privada para fazer a leitura da mensagem.

CARUSO & STEFFEN (2006) fazem uma analogia comparando a chave pública como um cadeado e a chave privada como a chave do cadeado, todos podem fechá-lo, porém só um terá a chave para abri-lo. TANEMBAUM (1999) deixa claro que quanto maior for o número criptográfico escolhido pelo emissor, maior será a dificuldade em quebrar o algoritmo, de fato, a fatoração de um número de 500 dígitos levaria 1025 anos. Em contrapartida, maior também, será o tempo gasto no processo de encriptação, o que às vezes, pode não ser satisfatório. CARUSO & STEFFEN (2006) prevêem que a única forma de quebrar a criptografia RSA, e todas as outras técnicas de chave assimétrica, seria com a entrada de operação dos computadores quânticos:

“Esses computadores terão velocidade de processamento milhões de vezes mais rápida do que os atuais computadores mais rápidos. Por possuírem (por enquanto teoricamente) a capacidade de realizar cálculos simultâneos, isso eliminaria a atual segurança de métodos de chave assimétrica, como o RSA, podendo realizar ataques de força bruta quase que instantaneamente.” (CARUSO & STEFFEN, 2006, p. 182).

Com base nisso, uma nova etapa em algoritmos de segurança está surgindo, será a criptografia quântica. Ao invés de utilizar métodos matemáticos para a geração de chaves, o novo conceito fará uso das propriedades físicas baseadas na mecânica quântica. Esta já é uma tecnologia conhecida nos laboratórios de pesquisa, entretanto, ainda sem perspectiva de uso em curto prazo, devido principalmente aos altíssimos custos envolvidos do processo de desenvolvimento.

Backup

O processo de backup consiste na realização de cópias de segurança de arquivos ou configurações.

A norma NBR ISO/IEC 17799 (2005, p. 48) afirma que o objetivo da realização de backups é “manter a integridade e disponibilidade da informação e dos recursos de processamento de informação”. Para tanto, a norma ainda trás alguns itens que devem ser considerados durante o processo:

- Definição da necessidade das cópias;
- Produção de registros das cópias efetuadas com documentação apropriada;
- As cópias de segurança sejam armazenadas em uma localidade remota com um nível apropriado de segurança;
- As mídias sejam testadas regularmente para garantir que elas são confiáveis;
- Em caso de confidencialidade dos dados, as cópias sejam criptografadas.

Devem ser feitas cópias de segurança de todos os trabalhos desenvolvidos nas estações dos usuários. CARUSO & STEFFEN (2006, p. 194) afirmam que “essa providência facilita a recuperação das informações, precavendo-se de algum dano ou sinistro nos arquivos originais”. Conforme SÊMOLA (2003), várias cópias do mesmo arquivo podem ser feitas, dependendo da sua criticidade para a continuidade dos negócios.