Informações corporativas, a evolução do ambiente computacional englobando o ciclo de vida da informação e CIDAL

Apresentar o conceito de segurança aplicado à informação corporativa, mostrando os motivos que justificam sua necessidade, além de explicar os conceitos de dados e informações e a necessidade de protegê-los durante o seu ciclo de vida. Conceituar a sigla CIDAL dentro do contexto de Segurança da Informação.

No início, as distâncias geográficas limitavam as atividades das organizações, porém, com o advento das redes de computadores essa barreira ficou para trás. A globalização formou as empresas intercontinentais e, com o advento das redes de computadores, a distância entre elas ficou a um click de um mouse.

A possibilidade de as empresas manipularem suas informações de forma cada vez mais rápida e organizada fez com que nesses últimos anos houvesse um aumento significativo na eficiência em seus processos internos. Com isso, aumentou-se o poder da tomada de decisão.

Em razão dessa dependência com relação à informação, ficou clara a necessidade de a empresa ter de implementar controles para garantir a sua sobrevivência e a sua competitividade.

Quando a informação ainda não estava no meio digital, os mecanismos utilizados para protegê-la eram muitos mais simples, pois bastava um armário com chaves e uma porta, e tudo já estava resolvido. Dessa forma, só teria acesso à informação as pessoas que possuíssem a chave da porta e do armário. Hoje em dia, em virtude de a maior parte das informações estar em meio digital, e praticamente ser invisível, fica difícil aplicar todos os controles necessários para protegê-la de todas as ameaças existentes.

A portabilidade que a informação conseguiu com o advento dos equipamentos móveis fez com que as fronteiras das organizações ficassem muito além do limite físico, que era sem dúvida muito mais fácil de gerenciar e controlar.

Podemos definir dados como todos os bits e bytes que o computador irá manipular durante a sua atividade. Quando esses dados estiverem manipulados e organizados de uma forma que possam ser interpretados por pessoas, teremos ai a famosa informação.

A informação seria então a interpretação humana que se tem a respeito de um determinado dado, pois, se alguém não consegue interpretar uma determinada informação, automaticamente ela se transforma em um dado, afinal não terá nenhum sentido e não poderá ser utilizada de uma forma satisfatória. Podemos também dizer que são os dados configurados de uma maneira adequada ao entendimento e à utilização pelo ser humano.

Dentro de uma empresa existem milhares de dados e informações que diariamente são manipulados pelos profissionais para que possam realizar suas atividades.

Uma tarefa árdua será implementar controles que possam permitir que as pessoas trabalhem com esses dados e informações de forma segura e ao mesmo tempo não causem impactos nas realizações de suas tarefas.

Informações corporativas e a segurança da informação

Quando um caminhoneiro sai para fazer uma viagem distante da sua base padrão, ele sempre observa alguns itens prioritários para que sua viagem possa ser realizada de forma segura e

tranquila.

Em algumas grandes organizações, existem as pessoas que são responsáveis por tomar conta da frota e deixar os equipamentos que serão utilizados pelos seus motoristas em perfeitas condições. Para isso, fazem uma série de manutenções preventivas e checagem baseadas em checklists, verificando se os principais componentes estão em bom funcionamento.

Esse caminhão passa por uma série de verificações, como: nível do combustível, pressão dos pneus, equipamentos de emergência, nível do óleo, condição dos motores, acionamentos elétricos e mecânicos.

Quando o motorista recebe o seu equipamento para o transporte, mesmo sabendo que já foi feita previamente uma vistoria por parte da equipe de apoio, ele verifica o seu freio, nível de gasolina, espelhos, cintos e outros que necessitam funcionar.

Essas ações realizadas por todos esses envolvidos são chamadas de providência da segurança, em que são checados os principais itens para que a pessoa se sinta segura e consiga realizar sua atividade tranquilamente.

Com base nesse cenário, podemos verificar que a segurança muitas vezes é vista como um sentimento (isso mesmo), as pessoas precisam se sentir seguras para que possam realizar as suas atividades.

Uma pessoa só cuida ou só toma conta de algo que, direta ou indiretamente, tenha algum significado para ela, e caso ocorra alguma situação de perda, ela sofre grande impacto.

Será que o mesmo cuidado existe com as informações corporativas que circulam nas redes das empresas? Da mesma forma, os funcionários das organizações deveriam estar conscientes e preparados para aplicar todos os cuidados necessários com relação à segurança.

Antigamente as empresas agiam de forma corretiva, ou seja, esperavam primeiramente o problema acontecer e a partir daí saiam apagando os incêndios. Felizmente, depois dos acontecimentos de 11 de setembro de 2001, em que ocorreram os ataques terroristas nos Estados Unidos da América, o comportamento em relação à segurança mudou.

As corporações

Os procedimentos de segurança aplicam-se a qualquer tipo de organização que utilize a tecnologia da informação para gerenciar parcial ou totalmente suas atividades, podendo ela ser:

- Uma empresa simples com um ou alguns microcomputadores sem estarem conectados entre si;
- Uma empresa de qualquer porte, com computadores interligados em rede e às vezes com acesso à internet ou parceiros de negócios;
- Um ambiente corporativo em que vários departamentos se interligam entre si e com o mundo, por meio de tecnologias e infraestrutura de redes;
- Um ambiente cooperativo onde a empresa interliga seus departamentos com seus parceiros (fornecedores, clientes, logística, revendas etc.).

Com o passar dos anos, ocorreu uma profunda transformação na realidade da utilização dos computadores dentro das organizações.

No principio, os computadores eram isolados e manipulavam os dados de forma individual e em computadores que naquela época eram conhecidos como de grande porte. O acesso a esses computadores era segregado e somente o pessoal técnico e qualificado conseguia entender o que se passava com aquelas gigantescas máquinas. Durante esse período a necessidade de segurança era apenas manter os curiosos longe desses ambientes, de forma a não causar nenhum problema físico por causa do acesso ou manipulação indevida. Dessa forma, a necessidade de segurança resumia-se apenas a colocar uma porta com chaves e todo o problema estaria resolvido.

Com o desenvolvimento tecnológico, os computadores foram diminuindo de tamanho e a sua utilização passou a ser feita por pessoas normais e que necessitavam dessas máquinas para realizarem as suas atividades diárias. As empresas começaram a utilizá-lo em larga escala e em conjunto com os computadores de grande porte (mainframes). Nesse cenário aumentaram-se as necessidades de segurança, pois, além de proteger os dados que anteriormente estavam centralizados nos computadores de grande porte, necessitavam agora proteger os dados e as informações que se encontravam dentro dos equipamentos dos usuários. Essa proteção era voltada a evitar o uso indevido ou até mesmo a destruição.

Como em um passe de mágica, os computadores começaram a se conectar entre si, possibilitando que as organizações pudessem compartilhar informações em tempo real e aumentando a capacidade produtiva e de geração de negócios.

Novamente, com a transformação do cenário dentro das organizações, ocorreu a necessidade de se pensar na segurança, mas dessa vez o que estava em jogo era o "negócio" da organização. Assim, o cenário mudou e a necessidade de segurança passou a ser deixar as informações sempre disponíveis para que as pessoas pudessem acessar e realizar as suas atividades a qualquer tempo e lugar. Além disso, o acesso a esses dados e informações deveria ser permitido apenas para os próprios donos, responsáveis pela informação, de forma que as pessoas que não tivessem essa autorização não pudessem acessar, mantendo assim a sua confidencialidade.

Como a maioria das transações que eram realizadas pelos computadores começaram a envolver dinheiro ou informações confidenciais, secretas e privadas, houve a necessidade de que fossem implementados controles para que elas não pudessem ser acessadas ou alteradas sem o consentimento das partes que estavam envolvidas. Os controles implementados deveriam garantir que as informações não tivessem sido alteradas durante os processos de comunicação dos equipamentos eletrônicos.

Em uma velocidade inacreditável foram acontecendo fatos marcantes na Tecnologia da Informação, que causaram grande impacto nas relações interpessoais, bem como nas relações das pessoas com as organizações. Novas ferramentas de comunicação, utilizando como meio a internet, vieram para facilitar as atividades das organizações e aumentar a sua produtividade.

As redes sociais invadiram as organizações e, além de benefícios, trouxeram grandes preocupações para os profissionais que tinham como função implementar os controles de segurança de forma que a organização não tivesse seus dados ou informações comprometidas.

Aliado ao desenvolvimento da tecnologia ocorreu o barateamento dos equipamentos de informática, o que permitiu que muitas pessoas tivessem acesso à tecnologia. O computador, assim como outros equipamentos, por exemplo, celular, Palm, Notebook, Tablet, viraram ferramentas de trabalho e passaram a estar presentes nas mesas dos trabalhadores.

As informações que antes estavam armazenadas em papéis e guardadas em armários de forma segura estão agora armazenadas em meios eletrônicos e distribuídas em várias partes da organização e, o que é pior, como uma maior insegurança "invisível".

As empresas estão cada vez mais conectadas e hoje o número de empresas que não possui um equipamento eletrônico utilizado para manipular suas informações é muito reduzido.

Reações pessoais aos procedimentos de segurança

A necessidade de adoção de procedimentos e mecanismos de segurança nas organizações provoca uma série de reações próprias do comportamento humano, pois algumas pessoas aceitam os controles que devem ser implementados e sabem que eles são necessários para que tenham maior segurança, mas a maioria das pessoas não gosta das restrições impostas pelos controles de segurança, pois muitas vezes eles interferem na liberdade de fazer algo a que já estavam acostumados. A implantação dos controles acarreta em uma demora a mais para a realização de algo que às vezes era realizado com um esforço menor. Basta ver o exemplo de uma pessoa que não necessitava de uma porta para entrar na sua residência e, em razão de um assalto, teve de colocar um portão com uma fechadura tetra na entrada da sua casa. Logo em seguida, teve de colocar um alarme digital que permitiria a passagem para o segundo nível da sua casa e depois a instalação de algumas câmeras e sensores de presença que, ao menor sinal de problema, dispariam e emitiriam um sinal sonoro.

Apenas nesse exemplo a pessoa teria que perder um determinado tempo para passar por todos esses controles até chegar à sala da sua casa, acarretando em uma inconveniente perda de tempo, além de ter que carregar chaves, lembrar-se da uma senha, não andar muito rápido para que o alarme tocasse.

A maioria das pessoas fica impaciente ao esperar por aprovação para entrar ou fazer algo em um determinado ambiente. Imagine isso quando uma pessoa tem que esperar para validar uma transação eletrônica que executará uma série de controles de segurança antes de efetivar a transação.

Talvez seja por isso que a maioria das pessoas não gosta muito dos controles de segurança, fato que pode justificar a imensa dificuldade que os profissionais de Segurança da informação encontram para implantar, com sucesso, técnicas e procedimentos que protejam as informações corporativas.

Agora que você já estudou esta aula, resolva os exercícios e verifique seu conhecimento.
Caso fique alguma dúvida, leve a questão ao Fórum e divida com seus colegas e professor.

A seguir, preencha a(s) lacuna(s) com a(s) palavra(s) adequada(s) às afirmações.

A seguir, preencha a(s) lacuna(s) com a(s) palavra(s) adequada(s) às afirmações.

Referências

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. *Política de Segurança da Informação*: guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2006.

NAKAMURA, Emílio Tissato; GEUS, Paulo. Lício de. *Segurança de redes em ambientes cooperativos*. São Paulo: Berkeley, 2002.

SÊMOLA, Marcos. *Gestão da Segurança da Informação*: uma visão executiva. Rio de Janeiro: Elsevier, 2003.