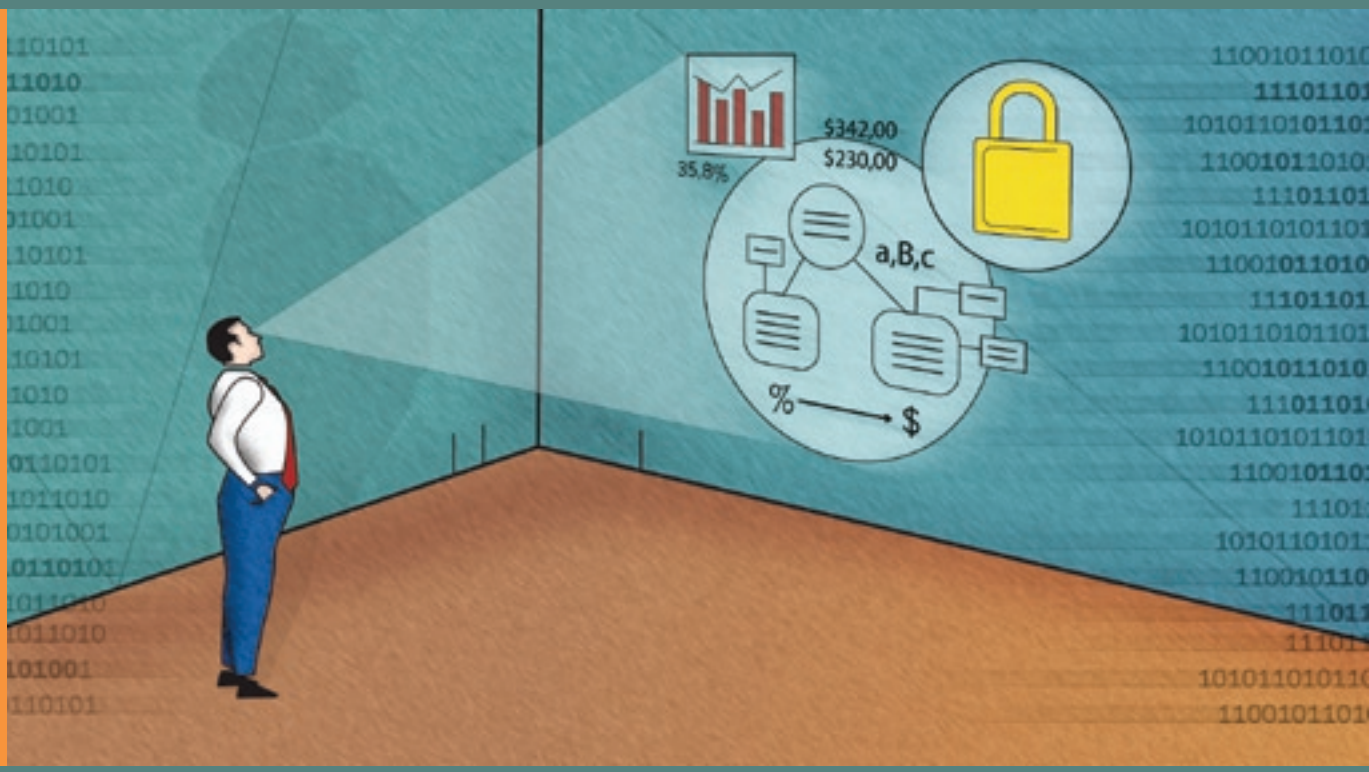
Segurança da Informação

Um diferencial determinante na competitividade das corporações



Promon

Business &
Technology
Review

Editorial

Nos dias de hoje, as empresas dependem cada vez mais dos sistemas de informação e da Internet para fazer negócios, não podendo se dar ao luxo de sofrer interrupções em suas operações. Um incidente de segurança pode impactar direta e negativamente as receitas de uma corporação, a confiança de seus clientes e o relacionamento com sua rede de parceiros e fornecedores.

Um incidente de segurança está diretamente relacionado com prejuízos financeiros, sejam eles devidos à parada de um sistema por conta de um vírus, ao furto de uma informação confidencial ou à perda de uma informação importante. Estima-se que worms *e vírus que atingiram grandes proporções de propagação – como, por exemplo, MyDoom, Slammer, Nimda – tenham ocasionado prejuízos da ordem de bilhões de dólares no mundo.*

Em última instância, um incidente pode impedir, direta ou indiretamente, a organização de cumprir sua missão e de gerar valor para o acionista. Essa perspectiva traz a segurança da informação para um patamar novo, não apenas relacionada com a esfera da tecnologia e das ferramentas necessárias para proteger a informação, mas também como um dos pilares de suporte à estratégia de negócio de uma corporação. A gestão da segurança assume, então, um novo significado, pois passa a levar em consideração os elementos estratégicos de uma organização e evolui para a extensão da prática de gestão de riscos do negócio.

Segurança da Informação

Um diferencial determinante na competitividade das corporações

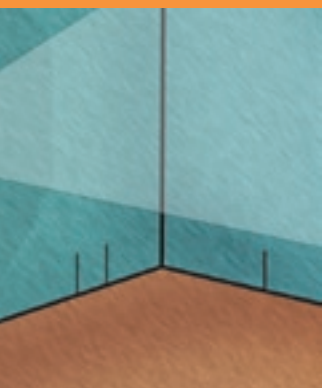
Cenário de ameaças e complexidade crescentes

Os incidentes de segurança da informação vêm aumentando consideravelmente ao longo dos últimos anos e assumem as formas mais variadas, como, por exemplo: infecção por vírus, acesso não autorizado, ataques *denial of service* contra redes e sistemas, furto de informação proprietária, invasão de sistemas, fraudes internas e externas, uso não autorizado de redes sem fio, entre outras.

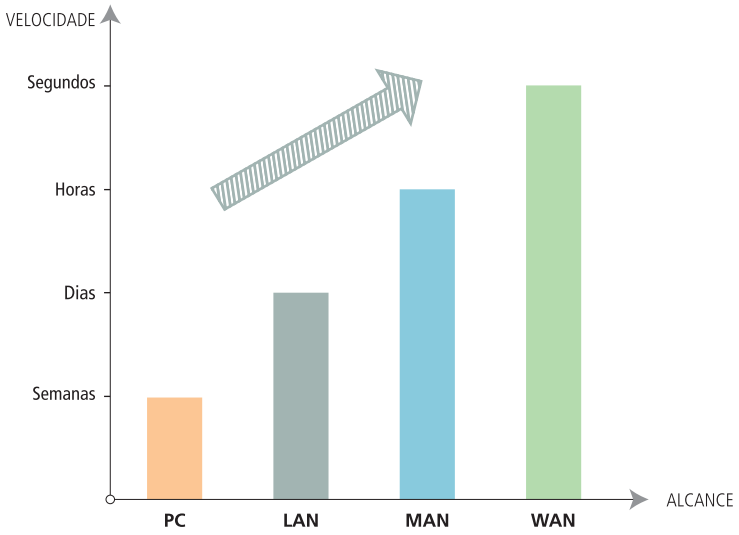
Um dos principais motivadores desse aumento é a difusão da Internet, que cresceu de alguns milhares de usuários no início da década de 1980 para centenas de milhões de usuários ao redor do globo nos dias de hoje. Ao mesmo tempo que colaborou com a democratização da informação e se tornou um canal *on-line* para fazer negócios, também viabilizou a atuação dos ladrões do mundo digital e a propagação de códigos maliciosos (vírus, *worms*, *trojans* etc.), *spam*, e outros inúmeros inconvenientes que colocam em risco a segurança de uma corporação. Além disso, a facilidade da realização de ataques através da Internet aumentou significativamente com a popularização de ferramental apropriado espalhado ao longo da rede mundial de computadores, habilitando desde *hackers* até leigos mal-intencionados a praticarem investidas contra sistemas de informação corporativos.

Juntamente com a difusão da Internet, outros fatores contribuíram para impulsionar o crescimento dos incidentes de segurança. Um desses fatores é o aumento do número de vulnerabilidades nos sistemas existentes, como, por exemplo, as brechas de segurança nos sistemas operacionais utilizados em servidores e estações de trabalho. Outro fator é o quão trabalhoso e custoso pode se tornar o processo de mitigar tais vulnerabilidades com a aplicação de correções do sistema, realizadas muitas vezes de forma manual e individual: de máquina em máquina. Por último, a complexidade e a sofisticação dos ataques também contribuíram de maneira direta para o aumento dos incidentes.

É a conjunção dessas condições que culmina, por exemplo, na parada generalizada de sistemas e redes corporativas ao redor do mundo, causada pela atuação de *worms* que se propagam pela Internet em questão de minutos. A tendência é que as ameaças à segurança continuem a crescer não apenas em ocorrência, mas também em velocidade, complexidade e alcance, tornando o processo de prevenção e de mitigação de incidentes cada vez mais difícil e sofisticado.



Crescimento na quantidade de ameaças



Não são apenas as ameaças externas que representam riscos a uma corporação. Os próprios funcionários representam alto risco quando mal-intencionados ou mesmo quando não conscientes dos riscos envolvidos na manipulação da informação. Dados de pesquisas apontam que mais de dois terços dos incidentes de segurança têm origem interna. Em contrapartida, é curioso notar que, em geral, o volume de investimentos destinados a minimizar a ocorrência desses incidentes, de causa interna, é significativamente menor do que os montantes destinados a prevenir ameaças externas. Surge, então, um desafio adicional na gestão da segurança de uma corporação: como garantir que os próprios colaboradores não se tornem causadores de incidentes de segurança? Como minimizar esses riscos?

Expansão contínua das fronteiras da segurança

As fronteiras da segurança se expandem, continuamente, na medida do avanço tecnológico. O universo de novas tecnologias evolui rapidamente e de formas até imprevisíveis. Essa evolução contínua coloca os executivos de segurança em uma posição desconfortável, tentando estabelecer controle sobre um alvo que se move e se modifica continuamente.

O aspecto mais curioso é que muitas das novas tecnologias à disposição dos usuários, quando utilizadas com os controles de segurança apropriados, são bastante valiosas como ferramenta de apoio aos negócios. Entretanto, quando funcionários incorporam essas tecnologias arbitrariamente em seu ambiente de trabalho, podem trazer ameaças desconhecidas à corporação. Alguns exemplos de tecnologias bastante populares utilizadas no escritório, mas que podem causar sérios danos quando usadas sem o devido cuidado ou de forma maliciosa, são:

Telefones celulares com câmera podem ser verdadeiras ameaças à segurança, dependendo da característica do negócio da empresa e, em geral, não estão conectados a nenhuma plataforma que a corporação possa controlar de maneira efetiva. Qualquer pessoa no ambiente de trabalho, mal-intencionada, pode utilizar, sem autorização, um telefone com câmera para tirar fotos de algo confidencial – por exemplo, um documento sigiloso, o protótipo de um produto ainda em desenvolvimento – e divulgá-las com a finalidade de lesar a corporação.

Dispositivos de armazenamento de dados portáveis constituem uma ameaça latente à segurança. É só conectar um dispositivo de memória do tamanho de um chaveiro na porta USB de uma estação de trabalho e qualquer informação que possa ser acessada pode ser copiada. Um funcionário mal-intencionado pode gravar quantidades significativas de informação confidencial da rede corporativa e sair tranqüilamente pela porta da frente sem que ninguém se dê conta. Não apenas dispositivos de memória portáteis constituem uma ameaça, mas também os MP3 *players*, celulares e PDAs, que ganham cada vez mais capacidade de armazenamento de dados.

Dispositivos sem fio cuja utilização cresce a cada dia, motivada, sobretudo, pela popularização da tecnologia WiFi presente em *laptops* e PDAs, abrem verdadeiras "janelas" nas redes corporativas. Torna-se cada vez mais barato e fácil configurar redes sem fio, de maneira não controlada, dentro de uma organização. Basta configurar um dispositivo sem fio como, por exemplo, um *laptop*, para funcionar como ponto de acesso e qualquer outro dispositivo não autorizado pode acessar a rede corporativa através dele. Detectar uma rede WiFi clandestina numa corporação é uma tarefa relativamente simples, diante do desafio de minimizar os riscos à segurança quando um funcionário acessa a rede corporativa, utilizando seu *laptop,* via uma rede sem fio fora de seu escritório, em um hotel ou aeroporto, por exemplo. Caso as medidas de segurança não estejam todas devidamente implantadas (ex.: utilização de *software* de criptografia, de formação de rede privativa e de *firewall* no *laptop*), ou caso o usuário não esteja devidamente consciente dos riscos envolvidos, ele pode expor a rede de sua corporação a qualquer curioso ou pessoa mal-intencionada que programe um dispositivo sem fio para capturar informações confidenciais.

Serviços *peer-to-peer* (ex.: transferência de arquivos, *instant messaging*, comunicadores VoIP) e ***web-based services*** (ex.: aplicações de acesso remoto) são categorias de aplicações bastante distintas, mas que guardam similaridades importantes no que diz respeito à segurança. Ambas podem ser facilmente instaladas pelos funcionários em suas estações de trabalho, possuem o apelo do aumento de produtividade e, em geral, burlam a infra-estrutura da segurança corporativa confundindo-se com o tráfego tradicional de Internet ou até com aplicações de negócio. Estas aplicações podem abrir acesso remoto às estações de trabalho, em que estão instaladas, e não permitem que a equipe de segurança tenha o devido controle das máquinas que estão acessando remotamente a rede corporativa. Dessa forma, podem ser utilizadas por usuários não autorizados e mal-intencionados para furtar informações confidenciais ou até disseminar vírus na rede.

O avanço tecnológico torna cada vez mais difícil a definição nítida de fronteiras para a organização. As corporações modernas estão cada vez mais conectadas ao ambiente que as circunda e permitem que terceiros do seu grupo de negócios – parceiros, fornecedores e clientes – também tenham acesso a seus ativos de informação, em intensidade comparável ao acesso fornecido a seus funcionários. Hoje, é possível acessar a rede e os sistemas de uma organização a partir de qualquer lugar do mundo com o auxílio da Internet, utilizando dispositivos variados, como *laptops* e PDAs, e meios de acesso distintos, como acesso WiFi ou conectividade banda larga residencial. Essas facilidades tornam a delimitação das fronteiras de uma corporação cada vez mais complexa, trazendo consigo uma fonte rica de vulnerabilidades, ameaças e riscos, introduzindo um nível de complexidade maior na gestão da segurança.

Engana-se quem pensa que as ameaças à segurança da informação estão relacionadas apenas com os sistemas e redes corporativas, conforme comentado até agora, numa área tipicamente denotada por segurança lógica ou digital. O conceito de segurança da informação vai muito além; pressupõe a identificação das diversas vulnerabilidades e a gestão dos riscos associados aos diversos ativos da informação de uma corporação, independentemente de sua forma ou meio em que são compartilhados ou armazenados, digital ou impresso. O objetivo da segurança é garantir a confidencialidade, a integridade e a disponibilidade desses ativos de informação de uma corporação.

As fronteiras da segurança da informação vão muito além da segurança lógica. Permeiam também a segurança física, que tem por objetivo prevenir acesso não autorizado, dano e interferência às informações, equipamentos e instalações físicas da organização. O campo da segurança física inclui a utilização de dispositivos que interagem com o mundo físico, em contraste e complementação aos dispositivos lógicos. Alguns exemplos desses dispositivos incluem câmeras de vídeo, catracas, sensores de presença, leitores de cartão de identificação.

Uma nova abordagem para a segurança

O impacto direto de incidentes de segurança nos resultados dos negócios, as crescentes e mais complexas ameaças, a expansão constante das fronteiras da segurança impulsionada pela tecnologia, além da necessidade de adequação a requisitos regulatórios, delineiam um novo cenário que está modificando as perspectivas tradicionais da segurança da informação. A evolução da segurança, como uma disciplina integrada, participante dos contextos operacionais e organizacionais, depende de abordagens e soluções que levam em consideração o novo modelo de organização dinâmica, distribuída e cada vez mais complexa.

A visão da segurança, com viés de soluções tecnológicas, voltada apenas para a área de TI das corporações, começa a mudar. Essa abordagem distorce a realidade de que os elementos produtivos da organização – pessoas, ativos e processos – são o foco real de uma estratégia de segurança. O assunto da segurança começa a tomar dimensões maiores em nível organizacional, compreendendo esforços mais abrangentes, com foco em gerenciamento de riscos ligado a objetivos mais amplos, como continuidade dos negócios, redução de custos com incidentes de segurança, aumento da competitividade e inevitáveis exigências legais e regulatórias. A segurança começa a ser percebida como um problema de negócio e não apenas de tecnologia.

Tais mudanças requerem muito mais do que uma abordagem reativa, pontual, sem embasamento de processos e dependente de esforços individuais. Requerem uma abordagem proativa, adaptativa, orientada a processos, em que a segurança é realmente gerenciada de forma continuada e sistemática, como um elemento "vivo".

Os gastos com segurança vêm crescendo, proporcionalmente, às expectativas de aumento do número e sofisticação das ameaças, e nem sempre existe a sensação de que a corporação está mais segura. A forma como esses gastos são encarados também passa por mudanças pois, tradicionalmente, as corporações enxergam segurança como uma despesa difícil de justificar. A justificativa usual, utilizada para viabilizar um projeto nessa área, é o aumento do nível de segurança, a expectativa de perda na ocorrência de problemas de segurança e a proteção contra riscos que não são claramente identificados e só são mensurados quando um incidente ocorre de fato. Essa abordagem torna difícil a priorização das iniciativas e a visualização dos benefícios trazidos por cada uma delas.

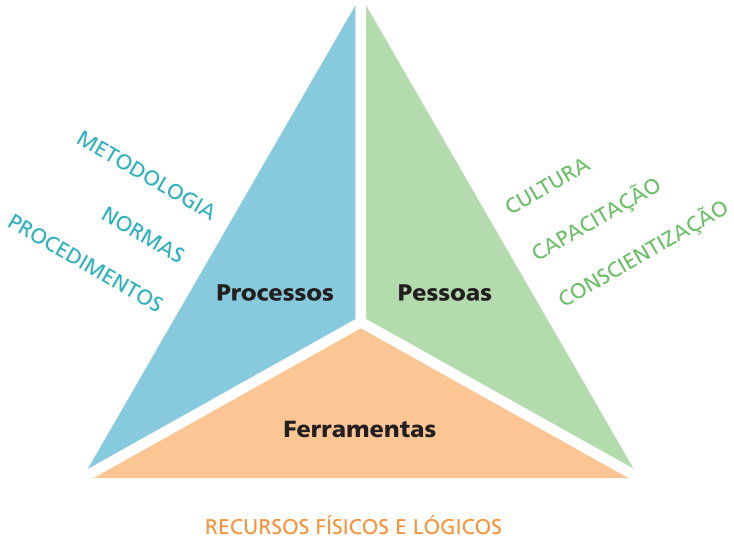
Da perspectiva financeira, a segurança começa a ser encarada, em muitas corporações, como investimentos que auxiliam a organização a atingir seus objetivos de negócio. Dessa forma, os gestores de segurança necessitam justificar investimentos com base em métricas financeiras, similar a outros investimentos da organização. Torna-se cada vez mais comum a adoção de métricas de avaliação de investimento, que levem em consideração os custos e benefícios associados a uma iniciativa de segurança, facilitando a tomada de decisão e a priorização das diversas iniciativas. Uma das métricas mais populares é o retorno sobre investimento – ROI (*Return on Investment*) – em que os benefícios são mensurados através de processos de avaliação de riscos e consistem, fundamentalmente, em custos que podem ser evitados, advindos de um possível incidente.

Todas essas mudanças levam à necessidade de um *framework,* como instrumento de gestão da segurança, em nível corporativo. Esse *framework* ampara as ações de uma corporação em diversos planos: pessoas, processos e ferramentas. A gestão da segurança é uma mistura desses três elementos, em que cada um deles é complementar e interdependente.

Pessoas: um dos elementos mais importantes na gestão da segurança, pois em essência são elas que executam e suportam os processos de uma corporação. Considera e trata os assuntos relacionados com as pessoas, seus papéis e responsabilidades na organização, indo desde a capacitação dos profissionais responsáveis pela segurança até a conscientização da organização como um todo.

Processos: constituem a linha mestra da gestão da segurança no dia-a-dia. Compreendem desde a visão da corporação, sua estratégia de segurança, a definição das políticas, até os processos que colocam em prática as políticas, os procedimentos, a documentação de controle e os padrões de conformidade. Através de processos bem definidos, uma corporação torna a segurança uma responsabilidade de todos e não apenas da equipe de segurança, pois determinam diretrizes do que é ou não permitido.

Ferramentas: são as soluções de segurança empregadas para suportar os processos delineados. São elas que facilitam a devida aplicação das políticas de segurança e seu monitoramento. Incluem diversas funcionalidades, desde a identificação dos usuários, criptografia de dados, defesa contra ameaças, até a gestão da segurança.



PESSOAS

O elo fraco da corrente da segurança da informação

A implantação de processos e ferramentas nem sempre é suficiente para garantir a segurança das informações. Sempre que a informação necessita ser manuseada por uma pessoa, ela está potencialmente em risco. À medida que as corporações permitem acesso mais abrangente e mais profundo às informações, os riscos de segurança aumentam exponencialmente com o número de usuários habilitados ao acesso.

Há diversos meios para mitigar riscos tecnológicos. Processos falhos podem ser detectados em auditorias ou verificações de rotina. Mas, como garantir que as pessoas estão trabalhando de maneira adequada? Deve-se monitorar as atividades das pessoas o tempo todo? Vale a pena criar controles e mais controles para eliminar possíveis vulnerabilidades?

A resposta mais viável, na maioria das vezes, é não. A melhor, e talvez única, maneira de garantir que as pessoas estejam trabalhando de modo seguro é conscientizá-las dessa necessidade. Riscos simples, como deixar papéis na impressora, fornecer informações por telefone ou deixar papéis com informações importantes em locais acessíveis, podem ser evitados conscientizando as pessoas do risco existente nesses comportamentos.

Não se pode prever todas as possibilidades de vulnerabilidades quando pessoas estão envolvidas. Não há como desenvolver um treinamento específico para cada ocasião em que a ação indevida de uma pessoa possa comprometer a segurança da empresa. Os treinamentos devem procurar enfatizar a postura que um profissional deve ter em relação a possíveis riscos.

Empresas adotam diferentes técnicas para tornar seus funcionários cientes dessa necessidade, como palestras educativas, treinamentos e folhetos. Algumas empresas adotam técnicas ainda mais ousadas, como afixar cartazes ou balões de gás nas mesas daqueles que violaram alguma regra comportamental de segurança.

O ideal é que todos entendam a necessidade de segurança e passem a se preocupar com esses aspectos em todas as situações do cotidiano. Uma pessoa consciente desses problemas, certamente, colabora para o aumento do nível de segurança corporativo. Pela conscientização e pelo treinamento, é possível transformar o elo mais fraco da cadeia, as pessoas, numa camada mais efetiva e forte na estratégia da segurança corporativa.

Mas, os desafios com relação às pessoas não se limitam à conscientização. A capacitação das equipes de segurança também representa um desafio importante para a gestão da segurança.

Devido à falta de padrões e à variedade de ferramentas e tecnologias existentes no mercado para amparar as práticas de segurança, manter uma equipe treinada e capaz de operar plataformas múltiplas torna-se um desafio. Além disso, a segurança da informação tem um caráter dinâmico intrínseco, derivado do surgimento de novas ameaças a cada dia, o que exige a atualização constante dos profissionais.

Além de capacitação técnica, cabe ressaltar que os integrantes de uma equipe de segurança necessitam de habilidades para aplicar políticas e processos no combate e prevenção de incidentes. Dessa forma, o conhecimento de processos torna-se importante no dia-a-dia e a capacitação em normas de segurança, como a ISO/IEC 17799, e de boas práticas de operação de tecnologia da informação, como o ITIL, garante aos profissionais de segurança uma bagagem valiosa para uma gestão eficiente.

Manter uma equipe de segurança atualizada e capacitada nas diversas disciplinas demanda tempo e recursos de uma corporação, sem mencionar a escassez de profissionais capacitados no mercado.

PROCESSOS

O controle da segurança da informação

Em tempos de grandes fraudes financeiras, que colocaram sob suspeita a credibilidade das informações contábeis, e de uma crescente dependência da tecnologia da informação nas empresas, deter uma certificação de segurança da informação é, certamente, um importante diferencial competitivo, que demonstra ao mercado a preocupação da empresa em manter suas informações confidenciais, íntegras e disponíveis.

Recentes leis e acordos internacionais, como a *Sarbanes-Oxley Act* e *Basiléia II*, demonstram a preocupação dos governos com fraudes e outros problemas relativos à confiabilidade e disponibilidade de informações, que podem colocar sob suspeita as ações de empresas. Alguns requisitos dessas leis referem-se nitidamente à segurança da informação, como a disponibilidade de informações de sistemas de informação (*logs*), garantia de não-repúdio de transações, sistemas menos suscetíveis a fraudes, segregação de funções e controle rígido de acesso.

Novas atribuições profissionais surgiram para suprir essa necessidade, como o CISO – *Chief Information Security Officer*, CSO – *Chief Security Officer*, funções normalmente encarregadas da gestão da segurança de uma corporação e das atividades de enquadramento das companhias às regulamentações de mercado. O papel desses profissionais tornou-se muito importante à medida que os sistemas de informação corporativos tornaram-se críticos e que os gestores da empresa passaram a ter responsabilidade cível sobre a precisão das informações corporativas.

Dessa maneira, nada mais natural que a busca de um padrão único e reconhecido de práticas para a segurança da informação e sistemas. A normalização e certificação de sistemas de gestão têm sido freqüentes e usuais como, por exemplo, as Normas de Qualidade (ISO 9001), Meio Ambiente (ISO 14001), Segurança do Trabalho (OHSAS 18001), entre diversas outras que atestam a adequação dos processos de uma empresa em relação aos requisitos de uma norma específica.

Nessa linha, o mercado reconhece a Norma ISO/IEC 17799 como a principal referência de melhores práticas para a gestão da segurança da informação. Essa norma teve como origem a BS 7799, da BSI – British Standards Institution, padrão britânico de segurança da informação e, ao contrário de outras normas ISO, como as séries ISO 9000 e ISO 14000, a ISO/IEC 17799 ainda não tem um guia de certificação. Atualmente, a certificação de segurança da informação somente é possível pela Norma BS 7799-2:2002.

Quando uma corporação adota a ISO/IEC 17799 como referência, ela adota naturalmente uma abordagem orientada para processos, que permite maior eficácia na gestão da segurança. Esse tipo de abordagem concentra-se nos processos que impactam diretamente os resultados do negócio, e não apenas em soluções tecnológicas que aumentam o nível de segurança. A corporação passa a avaliar e gerenciar os riscos inerentes a cada processo de negócio, e a segurança passa a ser incorporada naturalmente na gestão dos processos.

A ISO/IEC 17799 define o conceito do Sistema de Gestão da Segurança da Informação (SGSI), que consiste num instrumento de gestão baseada no gerenciamento de risco para estabelecer, implementar, operar, monitorar de forma proativa, revisar, manter e otimizar a segurança da informação de uma organização. O SGSI não é uma ferramenta tecnológica, como o nome pode levar a crer; é um instrumento completo de gestão que inclui, por exemplo, definição da estrutura organizacional, definição de papéis e políticas de segurança. Há o consenso do mercado de que a criação de SGSI, por si só, não resolve absolutamente todos os problemas de segurança existentes na empresa: apenas trata de sistematizar a gestão de riscos e descrever as melhores práticas para tratá-los.

Considerando esse quadro, a Norma ISO/IEC 17799 tem como principal característica descrever controles preventivos, em sua grande maioria, evitando a ocorrência de incidentes envolvendo as informações corporativas. Há também controles de monitoramento, visando reduzir o tempo de exposição ao risco, que permitem detectar, de maneira mais rápida e efetiva, eventuais violações às regras do Sistema.

Na documentação de um SGSI, existem três níveis de abstração que definem algumas dimensões da gestão da segurança: políticas, processos e procedimentos. Uma política deve descrever o entendimento, diretrizes e objetivos da empresa com relação à segurança da informação. Essa política deve ser simples o suficiente para ser facilmente compreendida por todos os colaboradores da empresa, e também genérica para que seja aplicável a toda a corporação.

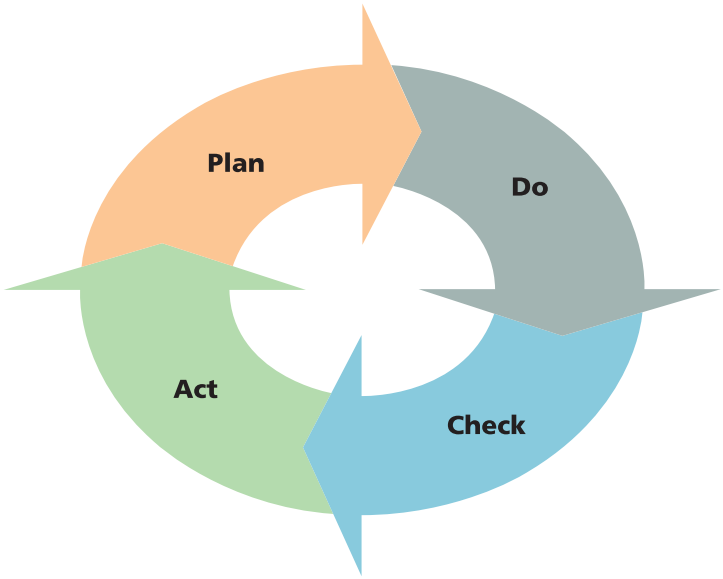
Uma política normalmente é implementada através de processos que descrevem quais atividades devem ser executadas para que uma tarefa seja cumprida. Podemos citar como exemplo o processo de cadastramento de um novo usuário: seria necessário criar uma conta de acesso à rede, criar uma conta de acesso no servidor de correio, permitir o acesso da pessoa nos ambientes físicos da empresa, cadastrar as permissões de acesso num determinado repositório da empresa e também os perfis nos aplicativos que tenha que utilizar.

Já um procedimento descreve os detalhes de uma determinada tarefa. Em geral, são instruções de trabalho que permitem que qualquer profissional, de formação e conhecimento similar, possa operacionalizar uma tarefa.

Dessa maneira, a criação de um Sistema de Gestão da Segurança da Informação se torna mais simples, dividindo as atividades em diferentes camadas, com diferentes níveis de detalhamento. A revisão de um procedimento de trabalho como, por exemplo, a troca da versão de um aplicativo, não precisa alterar processos e políticas corporativas. Normalmente, o mercado se refere ao conjunto de políticas, processos e procedimentos como "Política de Segurança".

Ao contrário do que se imagina, a ISO/IEC 17799 não descreve apenas práticas para a gestão da segurança da informação em TI, mas em várias outras áreas, como o controle físico de acesso, a segurança de equipamentos de escritório (fax, copiadoras etc.), a documentação de processos de trabalho, os critérios para o aceite de serviços terceirizados e manuseio de documentos, entre diversas outras.

Dessa maneira, a norma sugere a implantação do Sistema de Gestão da Segurança da Informação de maneira similar aos já conhecidos Sistemas de Gestão da Qualidade e Meio Ambiente, pelo ciclo contínuo de aprimoramento do Sistema. Esse ciclo, conhecido como PDCA (*Plan – Do – Check – Act*) é implementado da seguinte maneira:



PLAN

Estabelecer um Sistema de Gestão de Segurança da Informação

- Definir uma diretriz para a segurança da informação em consonância com os objetivos de negócio da corporação.
- Realizar um levantamento de todos os ativos de informação contidos na empresa.
- Atribuir um valor para cada ativo, conhecer suas vulnerabilidades e ameaças e o impacto associado a cada ameaça.
- Definir, de acordo com as práticas da norma, quais controles devem ser introduzidos para reduzir o risco existente.

DO

Implementar e operar o Sistema de Gestão da Segurança da Informação

- Definir planos de tratamento de riscos, que podem incluir a instalação de ferramentas, treinamentos, campanhas de conscientização, criação de procedimentos de trabalho, ou transferir o risco para terceiros (contratação de seguros).

CHECK

Monitorar e revisar o Sistema de Gestão da Segurança da Informação

- Verificar se, no tratamento dos riscos identificados, os planos delineados foram adequados.
- Verificar se o Sistema está atingindo os objetivos esperados.

ACT

Manter e melhorar o Sistema de Gestão da Segurança da Informação

- Verificar a adequação do Sistema de Gestão da Segurança da Informação em relação aos objetivos iniciais.
- Propor melhorias do Sistema.
- Definir novos objetivos de segurança.

A Norma ISO/IEC 17799 pode ser aplicada em qualquer processo ou âmbito de uma empresa. A situação ideal é iniciar a implantação de um Sistema de Gestão da Segurança da Informação num âmbito reduzido e, com o amadurecer do sistema, expandir sua abrangência para outras áreas.

A tendência é que a Norma ISO/IEC 17799 tenha rápida expansão, no médio prazo, e que venha a se tornar uma exigência comum para a contratação de serviços ou até mesmo para a análise do risco financeiro de uma companhia. Até o final de 2005, mais de 1800 companhias deverão receber seus certificados e outras dezenas de milhares já estarão trabalhando conforme os preceitos dessa norma.

Uma nova revisão da ISO/IEC 17799 está em andamento, devendo incluir os requisitos para a certificação e tendo sua numeração alterada para ISO/IEC 27001. Uma vez que a certificação é feita somente pela norma britânica BS 7799-2:2002, a disponibilização de uma versão ISO certamente irá estimular as empresas a certificarem seus sistemas de gestão da segurança da informação.

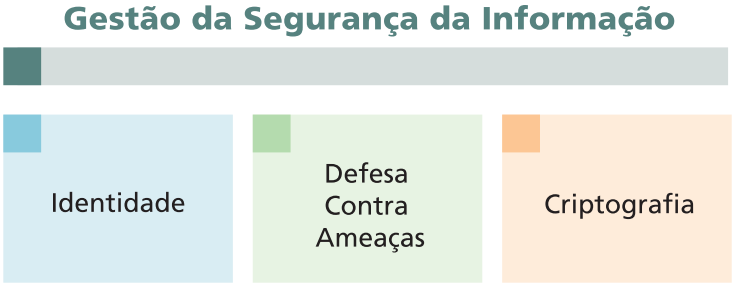
Espera-se que essa nova versão não tenha mudanças significativas em relação à versão atual da norma (ISO/IEC 17799:2005). A transferência dos certificados já emitidos, segundo os critérios da BS 7799-2:2002, será gradual.

FERRAMENTAS

Facilitadoras da gestão da segurança da informação

Mais do que processos de trabalho bem definidos, profissionais conscientes e capacitados, a segurança da informação requer ferramentas específicas para a implementação das regras contidas nas políticas de segurança. Muitos dos requisitos de controle e prevenção somente podem ser conseguidos com o uso de soluções de *hardware* e *software*. Por exemplo: a aplicação de uma política de acesso, para ser implementada, depende invariavelmente de *firewalls*, servidores de autenticação, equipamentos de rede.

Atualmente, um executivo de segurança da informação tem, à sua disposição, um arsenal de ferramentas sem igual para garantir a segurança dos ativos de uma corporação. Os principais blocos de soluções estão enumerados a seguir:



GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Soluções que permitem a gestão da segurança de maneira centralizada e fazem parte de uma categoria denominada SIM (*Security Information Management*). Existem dois grupos de funcionalidades que podem residir em uma ou em mais ferramentas:

Monitoramento

Realizam a análise e correlação de eventos originados em diversos sistemas através de uma plataforma única, e permitem a análise forense de incidentes, oferecendo um painel de bordo às equipes de segurança.

Configuração e administração

Permitem a verificação e a modificação de configuração de diversas plataformas e sistemas de maneira a garantirem a conformidade com as políticas de segurança. Como exemplos de atividades realizadas por essas ferramentas podemos citar a modificação de uma regra num *firewall,* ou a verificação das versões dos aplicativos, instalados nas estações de trabalho, para identificar a necessidade de atualizações.

GESTÃO DE IDENTIDADE

Ferramentas que permitem a correta identificação de um usuário para lhe conferir acesso de acordo com seu perfil.

Identificação/Autenticação

Permitem identificar unicamente um usuário e verificar a autenticidade da sua identidade através de mecanismos variados, como, por exemplo, senhas pré-definidas, certificados digitais, biometria ou dispositivos portáteis (*tokens, smart cards*).

Autorização/Controle de acesso

Possibilitam especificar as ações permitidas e níveis de privilégio diferenciados para cada usuário através do estabelecimento de políticas de uso.

Public Key Infrastructure/Certification Authority

Realizam a geração e gestão de chaves e certificados digitais que conferem autenticidade aos usuários ou à informação. Outra aplicação dessa categoria de ferramentas é o fornecimento de chaves para suportar soluções de criptografia.

DEFESA CONTRA AMEAÇAS

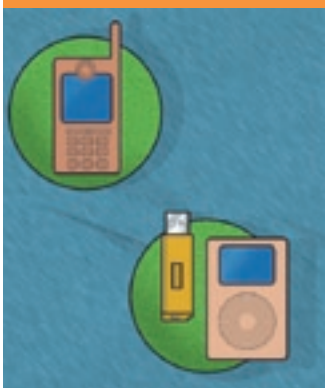
Diversas soluções atuando, de forma preventiva ou corretiva, na defesa contra ameaças à segurança de uma corporação.

Proteção de perímetro

Permitem definir uma fronteira, lógica ou física, em torno de um conjunto de ativos de informação e implementar as medidas necessárias para evitar a troca de informação não autorizada através do perímetro. Os *firewalls* representam as soluções mais comuns de proteção de perímetro, podendo realizar inspeção e filtragem de pacotes de dados, analisando as diversas camadas até o nível da aplicação. Existem dois tipos de *firewalls*: os tradicionais *appliances* de segurança instalados na rede ou os *personal firewalls* que podem ser instalados em estações de trabalho ou servidores.

Detecção de anomalias e intrusão

Realizam o monitoramento de redes, plataformas e aplicações visando a detecção de atividades não autorizadas, ataques, mau uso e outras anomalias de origem interna ou externa. Empregam métodos sofisticados de detecção que variam desde o reconhecimento de assinaturas, que identificam padrões de ataques conhecidos, até a constatação de desvios nos padrões de uso habituais dos recursos de informação. Os *Intrusion Detection Systems* (*IDS*) são as ferramentas mais utilizadas nesse contexto e atuam de maneira passiva, sem realizar o bloqueio de um ataque, podendo atuar em conjunto com outros elementos (ex.: *firewalls*) para que eles realizem o bloqueio. Uma evolução dos IDS são os *Intrusion Prevention Systems* (*IPS*), elementos ativos que possuem a capacidade de intervir e bloquear ataques. Tanto IDS como IPS podem existir na forma de *appliances* de segurança, instalados na rede, ou na forma de *host IDS/IPS*, que podem ser instalados nas estações de trabalho e servidores. Outras ferramentas importantes nesta categoria são os *Network Behaviour Anomaly Detectors* (*NBAD*) que, espalhados ao longo da rede, utilizam informações de perfil de tráfego dos diversos roteadores e *switches* para imediatamente detectar ataques desconhecidos, ataques distribuídos (*Distributed Denial of Service – DDoS*) e propagação de *worms*.



Proteção contra infecção

Garantem que os sistemas e os recursos de informação neles contidos não sejam contaminados. Incluem, principalmente, os antivírus e filtros de conteúdo. Os antivírus ganham cada vez mais sofisticação, realizando a detecção e combate de ameaças que vão além dos vírus, incluindo *trojans*, *worms*, *spyware* e *adware*. Os filtros de conteúdo aplicam políticas de utilização da *web*, examinando conteúdo consumido durante a navegação (ex.: programas executáveis, *plug-ins*). Existem também os filtros de conteúdo voltados para *e-mails*, chamados ferramentas *anti-spam*. As ferramentas de proteção contra infecção são instaladas tipicamente nas estações de trabalho e servidores, mas já existem versões voltadas para a rede, ou seja, eliminam ameaças antes de chegarem ao usuário, bloqueando na própria rede os pacotes infectados.

Identificação de vulnerabilidades

Ferramentas utilizadas pelos profissionais de segurança para identificar vulnerabilidades nos sistemas existentes (*vulnerability scanners*). Realizam uma varredura nos sistemas em busca de falhas de segurança, a partir de uma base de conhecimento de vulnerabilidades existentes em elementos de rede, sistemas e aplicações.

Backup/recovery

Permitem o *backup*, de forma automatizada, de informações contidas em estações de trabalho e servidores. Além disso, possuem funcionalidades de recuperação e restauração de informações perdidas em caso de incidentes.

CRIPTOGRAFIA DAS INFORMAÇÕES

Mecanismos que garantem a confidencialidade da informação em diversas camadas, através da aplicação de algoritmos de criptografia. Variam desde a criptografia das informações gravadas em dispositivos de memória (ex.: discos rígidos, *storage*) até criptografia das informações em trânsito visando à comunicação segura. Os equipamentos mais conhecidos para a comunicação segura são os chamados concentradores de VPN (*Virtual Private Networks*), que permitem a formação de redes virtuais seguras nas quais todo o tráfego trocado (entre dois nós de rede – *site-to-site* – ou entre uma estação remota e um nó de rede – *client-to-site*) é criptografado utilizando algoritmos como o IPSec ou, mais recentemente, o SSL (*Security Socket Layer*).

As soluções para segurança experimentam uma fase de intensa inovação tecnológica e de crescente sofisticação motivadas, principalmente, pelo aumento constante das atividades maliciosas. É um mercado aquecido, haja vista os crescentes investimentos das corporações em soluções para aumentar seus níveis de segurança.

O mercado de soluções de segurança é relativamente novo e apresenta um elevado nível de fragmentação. Nele coexistem diversas empresas, oferecendo soluções para cada uma das áreas ilustradas, e que se destinam, muitas vezes, apenas parte do problema. Exemplos de soluções pontuais são os *firewalls* e antivírus presentes na quase totalidade das corporações. A diversidade de soluções isoladas representa desafios de interoperabilidade, integração e gerenciamento para as equipes de segurança.

Com a mudança de sua visão sobre segurança, as corporações começam a demandar soluções mais abrangentes, com foco na prevenção de ameaças, em vez de soluções pontuais voltadas para a detecção de ameaças. Além da preocupação com tecnologia, as corporações começam a incorporar a necessidade de gerenciar processos e pessoas através das ferramentas. Como resultado das necessidades dos clientes, o mercado de soluções de segurança aponta para sua consolidação, com o surgimento de empresas que oferecem soluções mais completas e abrangentes, que passam a visar de forma única e integrada à maior parte das necessidades de segurança de uma corporação. O intenso movimento de fusões e aquisições no mercado de segurança é um dos indicadores da consolidação.

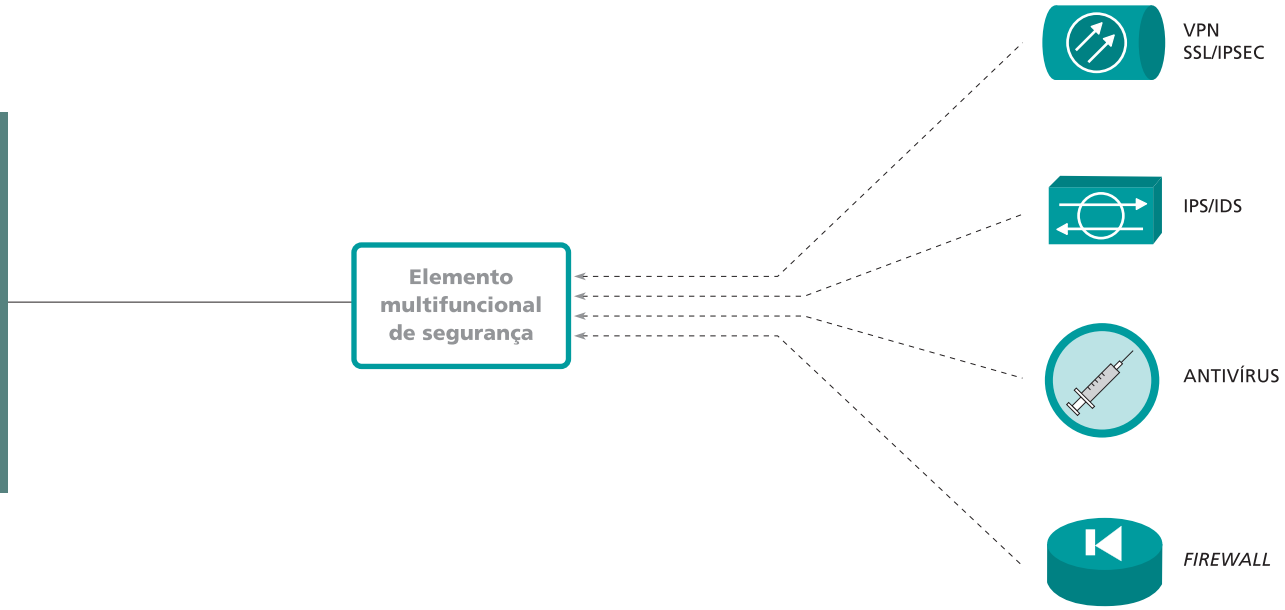
Em meio à crescente sofisticação das soluções de segurança, algumas tendências vêm ganhando destaque e devem marcar os próximos passos do desenvolvimento de novas ferramentas. A primeira delas é a utilização de ferramentas que congregam diversas funcionalidades de segurança em um elemento único, os elementos de segurança multifuncionais. A segunda tendência é a integração da segurança nos elementos de rede. Por último, podemos ressaltar também a crescente importância de ferramentas de gestão da segurança.

ELEMENTOS DE SEGURANÇA MULTIFUNCIONAIS

Os primeiros produtos de segurança foram criados a partir de ferramentas customizadas e especializadas para funcionalidades de segurança como, por exemplo, combater ataques de *hackers* ocorridos numa conexão da Internet. Foi assim que surgiram os primeiros *firewalls* como elementos dedicados à segurança. Outros produtos específicos surgiram no intento de fortalecer a segurança das redes e sistemas corporativos. É o caso dos concentradores de VPN, que permitem a formação de redes seguras.

As soluções de *firewall* e VPN surgiram, originalmente, na forma de *appliances* dedicados e supriam as necessidades das grandes corporações, mas eram considerados caros e pouco adequados no contexto das pequenas e médias corporações.

Os produtos de *firewall*/VPN amadureceram, tornaram-se mais sofisticados em suas funcionalidades nativas e passaram a incorporar novas funções, dando origem a uma nova categoria de produtos, a dos elementos multifuncionais de segurança, também conhecidos como soluções de *Unified Threat Management* (UTM). Esses elementos são definidos pela combinação inteligente de funcionalidades de segurança numa instância única de *hardware* e *software*. O principal objetivo de tais elementos é



garantir a segurança de maneira mais abrangente, permitindo a identificação e mitigação de ameaças diversas, desde a camada de rede até a aplicação. Pelo fato de concentrarem diversas funcionalidades em um elemento único, propiciam uma grande facilidade no gerenciamento da segurança, feito remotamente, a partir de centros de operações especializados (SOC – *Security Operations Centers*).

As novas gerações desses produtos incorporam diversas funcionalidades, passando por filtragem de tráfego (*firewall*), comunicação segura (VPN), detecção e prevenção de intrusão (IDS/IPS), antivírus/*anti-spam*, filtro de conteúdo, autenticação e controle de acesso. Nem todas essas funcionalidades precisam estar ativas ao mesmo tempo e o usuário pode selecionar as funcionalidades que deseja, de acordo com suas necessidades.

As principais vantagens das soluções multifuncionais residem no menor custo, quando comparadas à soma das soluções individuais, menor complexidade, maior facilidade de gerenciamento e interoperabilidade garantida entre as diversas funções incorporadas pelo produto. A expressão mais tangível desses benefícios é a redução do custo total de propriedade (TCO – *Total Cost of Ownership*), que envolve desde o investimento na aquisição da solução até os custos de instalação, operação e manutenção.

A decisão da utilização de elementos multifuncionais, nos variados contextos de uma corporação, depende da análise do nível de desempenho requerido em relação às funcionalidades desejadas. Não existem soluções prontas, que sirvam a toda e qualquer corporação. As características da topologia de uma rede corporativa ou o tamanho da corporação determinarão a utilização, ou não, desse tipo de solução. Existem casos em que o nível de desempenho requerido é extremo como, por exemplo, na proteção de *data centers* de grandes corporações. Nesses casos, elementos de segurança dedicados a uma única função podem ser mais indicados, pois não compartilham recursos com funcionalidades adicionais. Em contrapartida, os elementos multifuncionais são bons candidatos para suprir as diversas necessidades de segurança de uma filial menor ou uma empresa de pequeno porte. A utilização de elementos multifuncionais dependerá da análise caso a caso.

SEGURANÇA INTEGRADA NA REDE

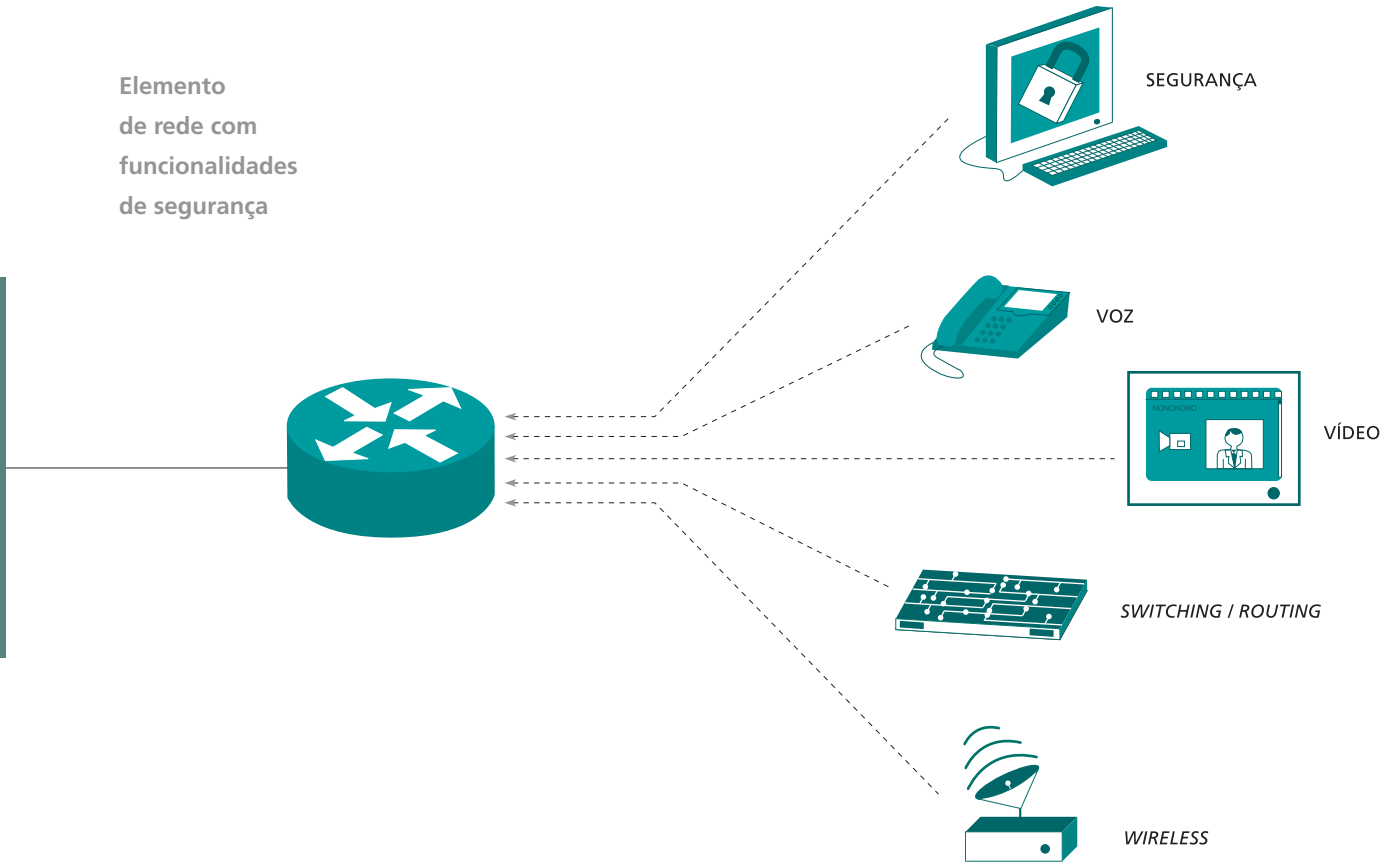
Enquanto observamos a sofisticação crescente de produtos especializados em segurança, integrando cada vez mais funcionalidades em um único produto, uma outra tendência se verifica na prática. É a integração cada vez maior das funcionalidades de segurança nos elementos de rede, sejam eles pertencentes a uma rede corporativa ou a uma rede de uma operadora de telecomunicações.

A segurança das redes vem se tornando cada vez mais importante. As redes convergentes transportam, hoje em dia, informações relevantes para todos os aspectos de um negócio, desde dados de extrema criticidade, como é o caso de informações financeiras, até a comunicação tradicional de voz, vídeo e dados. Além de desempenharem sua funcionalidade tradicional de comunicação, as redes passam a ter também um papel de destaque no combate a ameaças à segurança dos dados e aplicações. Um exemplo disso é a incorporação das funcionalidades de segurança nos roteadores de um *backbone* de uma rede IP, que podem identificar e mitigar ataques antes que tornem indisponível um nó da rede ou atinjam as estações de trabalho.

As abordagens tradicionais de segurança de redes tinham como referencial o modelo de "fortaleza", com a utilização de *firewalls* e outras tecnologias para manter todos fora da rede, com exceção dos usuários autorizados. Entretanto, essa abordagem é desafiada pela mudança dos requisitos de negócios, que demandam cada vez mais uma forma de acesso pervasivo, ou seja, acesso a qualquer hora, em qualquer lugar, por diversos tipos de usuários, incluindo funcionários e terceiros. A mobilidade, as tecnologias sem fio e o avanço da Internet colaboram para a viabilização desse acesso pervasivo, que pode servir de canalizador para novas ameaças, ataques ou até a utilização de recursos por pessoas não autorizadas. Soma-se a isso o fato de que ameaças residem também dentro da corporação, em usuários mal-intencionados, e não apenas na figura de *hackers* espalhados pela Internet.

Dessa forma, as novas redes precisam incorporar a capacidade de responder às diversas ameaças de segurança de maneira que continuem disponíveis e confiáveis, sem impactar as atividades de negócios de uma corporação. As redes passam a interagir com diversos elementos de segurança (desde *appliances* com funcionalidade única a elementos multifuncionais de segurança – ex.: *firewall* e IDS/IPS – até soluções de segurança dos *endpoints* – ex.: antivírus, anti-*spyware*, *host IDS/IPS*, *personal firewall*), de maneira integrada e colaborativa, fazendo parte de uma solução de defesa abrangente, que percorre as diversas camadas até a aplicação. O conceito de integração da segurança na rede é também conhecido por *network-based security*.

Um exemplo dessa abordagem colaborativa é o mecanismo de controle de admissão de usuários na rede, que ganha um papel importante no contexto de redes corporativas pervasivas. Esse mecanismo garante que apenas os usuários que estejam em conformidade com as políticas de segurança tenham acesso à rede e previne que dispositivos infectados, ou não confiáveis, se conectem à rede. Para isso, é necessário que os elementos de rede interajam com os aplicativos de segurança instalados no dispositivo que solicita permissão de conexão à rede, e façam verificação a partir de critérios pré-definidos, por exemplo, se o dispositivo está com a versão do antivírus atualizado. Esforços de padronização e interoperabilidade entre diversos fornecedores são realizados para fomentar a difusão do conceito de



controle de admissão. Por exemplo: o IEEE 802.1x (*Port Based Network Access Control*) é um padrão estabelecido e incorporado em equipamentos de rede mais recentes, que permite a aplicação de políticas de controle de acesso de rede de forma interoperável, envolvendo equipamentos de fabricantes distintos.

A utilização da rede como uma ferramenta de segurança é também motivada pelos ataques cada vez mais sofisticados, que levam à adoção de uma abordagem "*defense in depth*" pelas corporações de maior porte, com a implementação de dispositivos de segurança, tanto nas estações de trabalho, como em servidores e também ao longo da rede. Dessa maneira, a corporação fica menos vulnerável e não depende apenas de poucos pontos de defesa, fazendo com que aumente a taxa de sucesso no combate às ameaças.

As pequenas e médias corporações possuem recursos mais limitados para infra-estrutura de TI e podem reduzir custos operacionais e investimentos ao adotarem plataformas integradas de rede e segurança. Dessa forma, empresas de menor porte podem alcançar um nível satisfatório de segurança de seus ativos de informação ao utilizaram roteadores de acesso que possuam funcionalidades de segurança.

As primeiras iniciativas no sentido da convergência de segurança e comunicação em elementos únicos ocorreram com a integração de módulos de *firewall* e VPN IPSec em roteadores. Entretanto, a adição de novas funcionalidades de segurança em elementos de rede não pára aí e inclui IDS/IPS, anti-DDoS, antivírus, *anti-spam*, filtro de conteúdo, controle de admissão/acesso de usuários. Os elementos de rede aos quais tais funcionalidades são integradas não se restringem apenas a *switches* e roteadores tradicionais, mas incluem também roteadores sem fio (com funcionalidade WiFi incorporada), expandindo ainda mais o conceito de integração.

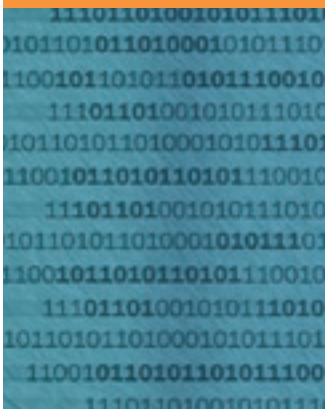
GESTÃO DA SEGURANÇA CENTRALIZADA

Outro desafio importante que as equipes de segurança enfrentam é a imensa quantidade de dados que precisam absorver para gerenciar a infra-estrutura de segurança corporativa. Cada solução gera, individualmente, uma quantidade bastante significativa de *logs* e alarmes, que precisam ser analisados para determinar se existe mesmo algo acontecendo de errado, por exemplo, algum ataque ou alguma infecção de vírus em massa.

Apesar de ocorrer a geração de um grande volume de dados pelas plataformas de segurança, somente uma pequena fração dos eventos se confirma como incidente e realmente afeta a corporação. Muitos dos alarmes não possuem significância real e, muitas vezes, não dizem respeito a nenhuma ocorrência relevante. Torna-se difícil para a equipe de segurança construir uma visão geral da situação do ambiente para colocar em prática as ações necessárias. É um caso análogo ao dos sistemas de suporte à decisão, que precisam manipular grande quantidade de massa de dados para extrair tendências relevantes para o negócio.

Muitas vezes, as corporações instalam a infra-estrutura de segurança, mas não realizam o devido monitoramento pela dificuldade de extrair os eventos realmente relevantes para a tomada de decisão. É comum a existência de *firewalls* e IDS que nunca tiveram seus *logs* analisados ou sequer extraídos, figurando apenas como mais uma barreira para os invasores, sem que deles se extraia todo o potencial de proteção.

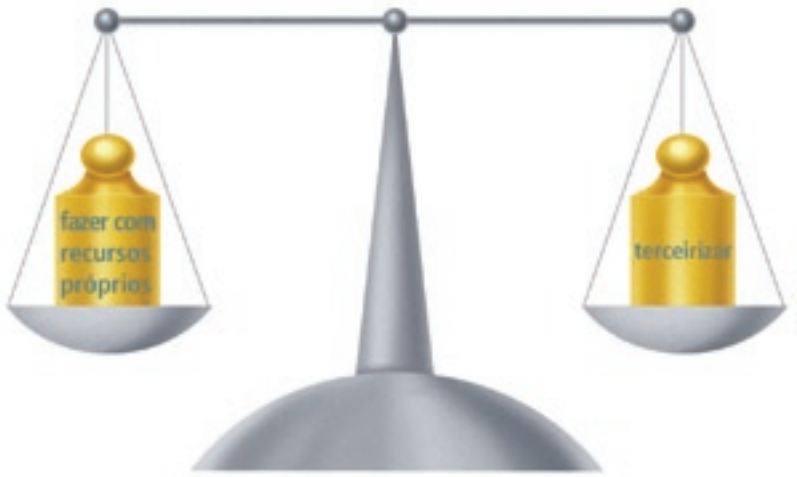
Tendo em vista o caráter estratégico conferido à segurança da informação nas corporações, faz-se necessário o acompanhamento e o monitoramento mais eficaz e em tempo real da infra-estrutura de segurança. Nesse contexto, surgem as ferramentas pertencentes a uma categoria denominada *Security Information Management* (SIM). São ferramentas capazes de coletar eventos de diversos elementos de segurança (ex.: *firewall*, IDS, antivírus, servidores de controle de acesso, *scanners* de vulnerabilidades etc.) e de rede (ex.: nível de processamento de roteadores e *switches*), normalizar, filtrar, correlacionar esses eventos utilizando algoritmos sofisticados, e então apresentar em tempo real os alarmes pertinentes ponderados por seu grau de severidade, através de uma interface centralizada. A partir de milhares de eventos, uma ferramenta SIM é capaz de indicar os alarmes realmente relevantes. Na ocorrência de um alarme, a ferramenta permite também o acesso aos dados históricos para identificação de um verdadeiro incidente de segurança.



As ferramentas SIM são capazes de centralizar a gestão da segurança da informação de uma corporação a ponto de criar um painel de bordo, com os indicadores relevantes ao dia-a-dia, da tomada de decisão de uma equipe de segurança. São inúmeros os benefícios associados a essa abordagem de gestão centralizada: redução de custos operacionais, aumento do nível de assertividade na detecção e mitigação de ameaças, facilidade de priorização de ações, diminuição do número de incidentes, diminuição de perdas financeiras e aumento do nível de segurança.

Além da coleta, correlação e apresentação dos dados para monitoramento, tais ferramentas estão evoluindo para um maior nível de automatização, mitigação de ataques e gestão de políticas de segurança de maneira que possam ser utilizadas também como ferramentas de auditoria e verificação de conformidade com políticas de segurança pré-estabelecidas. Vale ressaltar que, por mais que o processo de monitoramento e contenção de ameaças se torne mais automatizado, a adoção da ferramenta nunca irá substituir o conhecimento, a percepção, a intuição da intervenção humana. É possível construir um sistema que detecte problemas, identifique as medidas necessárias para corrigi-los e alerte o operador, que poderá desprezar o alerta ou tomar alguma medida corretiva em relação a ele. A contribuição humana também é muito valiosa na programação e no ajuste dos sistemas de gestão de segurança, de maneira que eles se tornem cada vez mais assertivos.

É importante lembrar que uma ferramenta SIM é um dos principais pilares sobre os quais se constrói um SOC (*Security Operations Center*). A espelho da função de um NOC (*Network Operations Center*) para uma rede de comunicação de dados, um SOC monitora e gerencia continuamente a infra-estrutura de segurança. A vertente de ferramentas necessárias para suportar um SOC é fortemente calcada numa ferramenta SIM para a prática do monitoramento. Os SOCs estão se tornando cada vez mais comuns devido à maior importância da segurança no contexto dos negócios. Corporações que possuem uma infra-estrutura de TI complexa e equipes dedicadas à segurança da informação são fortes candidatas a adotarem em seus SOCs ferramentas desse gênero. As operadoras de telecomunicações também se colocam na condição de usuárias de ferramentas SIM devido às necessidades de gerenciamento de sua infra-estrutura de prestação de serviços de telecomunicações, de ativos de clientes e de sua infra-estrutura de TI corporativa. Os provedores de serviços de segurança gerenciada, de um modo geral, também são considerados usuários potenciais dessas ferramentas para gerenciarem em tempo real os ativos de segurança de seus diversos clientes.



Terceirização em segurança

O fenômeno da terceirização já é algo bem conhecido no domínio da tecnologia da informação. A terceirização de TI e de outros processos de suporte é uma tendência em boa parte das corporações. Ultimamente, a segurança também começa a fazer parte da agenda da terceirização. Num primeiro momento, segurança da informação nos remete a um assunto bastante íntimo de uma organização e de extrema criticidade, tornando difícil imaginar qualquer extensão de terceirização das atividades relacionadas com segurança.

Entretanto, esse paradigma vem mudando progressivamente e os serviços de terceirização já são uma realidade para a segurança, em especial na Europa e Estados Unidos. Aspectos regulatórios, a crescente sofisticação e proliferação das ameaças de segurança requerem atualização constante das equipes, conhecimento mais especializado e monitoramento contínuo para minimizar as conseqüências derivadas de tais ameaças. Nem sempre as corporações possuem recursos e habilidades suficientes à prática da segurança para endereçar essas necessidades e passam, então, a considerar a terceirização de atividades relacionadas com segurança.

Para atender as necessidades das corporações, surgiram os diversos serviços de segurança gerenciada (*Managed Security Services* – MSS), que incluem:

- monitoramento contínuo (24x7) da infra-estrutura de segurança de uma corporação, da qual são extraídos eventos que dão origem às indicações de potenciais incidentes de segurança;
- configuração dos componentes da infra-estrutura de segurança;
- prevenção e correção de incidentes;
- análise de vulnerabilidade e testes de penetração.

Em vez de investir em soluções de segurança e manter uma equipe especializada para gerenciá-las, uma corporação pode contratar o serviço de segurança de um terceiro. A cobrança dos serviços gerenciados ocorre na forma de uma tarifa periódica, por exemplo, uma tarifa mensal que inclui desde os serviços prestados até o aluguel ou *leasing* da infra-estrutura de segurança, quando aplicável.

Além dos serviços gerenciados propriamente ditos, a oferta pode vir precedida por serviços profissionais voltados para o projeto e implementação da infra-estrutura a ser gerenciada, ou por serviços voltados para a definição de políticas ou adequação de processos de segurança.

A oferta de serviços gerenciados constitui um mercado relativamente novo e vem apresentando taxas de crescimento bastante expressivas nos últimos anos. Nesse mercado figuram empresas de múltiplas origens:

Pure-players: empresas bastante especializadas que se dedicam unicamente à oferta de serviços de segurança gerenciada.

Consultoria e integradores de sistemas: adicionam serviços gerenciados como um complemento de sua oferta tradicional de consultoria e integração de sistemas de segurança.

Fornecedores de soluções de segurança: oferecem serviços de gerenciamento em conjunto com as soluções que fornecem (ex.: antivírus, *firewall*, IDS).

***Outsourcers* de TI**: muitas vezes o gerenciamento da infra-estrutura de segurança já faz parte dos contratos de terceirização de TI.

Operadoras de telecomunicações: como forma de diferenciação, as operadoras, progressivamente, oferecem serviços de segurança gerenciada em adição aos serviços tradicionais de comunicação de dados.

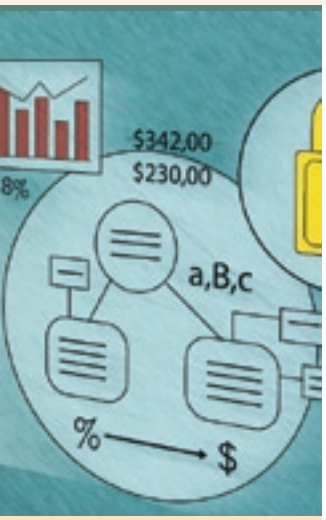
Os prestadores de serviços de segurança gerenciada contam com a infra-estrutura de um *Security Operations Center* (SOC) equipado com políticas e processos bem definidos, profissionais capacitados e ferramental adequado para suportar o gerenciamento remoto da infra-estrutura. Além de contarem com todo o ferramental do SOC, os provedores de serviços utilizam soluções de segurança instaladas nas dependências do cliente para detecção e mitigação das ameaças. Ao lado dos tradicionais *appliances* de segurança dedicados a uma função específica, os elementos multifuncionais e elementos de rede com funcionalidades de segurança integradas estão sendo cada vez mais empregados devido às suas vantagens de custo e facilidade de gerenciamento.

Até a terceirização completa da segurança de uma corporação, existe um gradiente de diversos serviços modulares que derivam das soluções a serem gerenciadas. É comum perceber no mercado a oferta modular orientada por soluções, por exemplo: VPN IPSec/SSL gerenciada, *firewall* gerenciado, IDS/IPS gerenciado, antivírus gerenciado, filtro de conteúdo gerenciado, anti-DDoS gerenciado e controle de acesso gerenciado, entre outros. Na contratação do serviço, o cliente tem a facilidade de escolher um ou mais componentes. As corporações podem se beneficiar dessa abordagem modular que lhes permite contratar os serviços de acordo com suas necessidades e disponibilidade de orçamento.

Além das grandes corporações, as PMEs (pequenas e médias empresas) começam a apresentar necessidades de segurança mais elaboradas e de monitoramento contínuo. Entretando, as empresas de menor porte têm recursos limitados para manter uma equipe dedicada ou investir em diversas soluções de segurança. O modelo de serviços gerenciados possibilita o aumento do nível de segurança dessas empresas em troca de uma tarifa mensal recorrente e previsível, ao invés de investimentos vultosos e de difícil viabilização.

Quando pensamos em terceirização da segurança, vários benefícios podem ser enumerados do ponto de vista de uma corporação.

Benefícios da terceirização de segurança



AUMENTO DO NÍVEL DE SEGURANÇA

- Acesso a maior *know-how* e *expertise*
- Capacidade de monitoramento 24x7x365
- Rede e sistemas atualizados constantemente em termos de segurança

REDUÇÃO DE CUSTOS

- Ganhos de economia de escala e escopo do provedor de serviços possibilitam menores custos para a corporação
- Diminuição de investimento em soluções de segurança (ex.: *firewalls*, IDS) oferecidas no modelo de terceirização pelo provedor de serviços
- Diminuição de custos com pessoal e demais procedimentos operacionais

FOCO EM ATIVIDADES PRINCIPAIS

- Possibilidade de reorientar esforços para o negócio principal, diminuindo o dispêndio de recursos em atividades de suporte

CONFORMIDADE REGULATÓRIA

- Facilitada, muitas vezes, pela contratação de provedor de serviços gerenciados

Apesar dos diversos benefícios trazidos pela terceirização, alguns desafios também são trazidos por ela e precisam ser considerados:

Acesso a informações confidenciais: o acesso de terceiros a informações confidenciais, como senhas dos *firewalls* e servidores, traz algumas indagações em relação à decisão de contratar um serviço gerenciado. Nessa hora, torna-se de fundamental importância a confiança no provedor de serviços, o controle dos níveis de acesso concedidos, a garantia de que as políticas de segurança do provedor com relação aos seus funcionários atendam aos requisitos da corporação, além de cláusulas contratuais que protejam a corporação de eventuais incidentes.

Dependência de terceiros: a diminuição do controle sobre os sistemas de segurança é outro fator que preocupa a corporação na decisão da terceirização, pois a torna dependente do provedor de serviços. Daí a importância de processos que possam ser auditados, permitindo a monitoração das atividades do provedor e garantindo o cumprimento das políticas de segurança estabelecidas. Ademais, é importante que a corporação tenha acesso à situação da infra-estrutura de segurança monitorada da forma mais transparente possível, através de relatórios em tempo real, e possa intervir em sua administração e controle. Os portais de relacionamento são de fundamental importância para oferecer transparência ao cliente final.

Definição de novas métricas de desempenho: numa primeira análise, é difícil determinar métricas para um acordo de nível de serviço (*Service Level Agreement* – SLA) de um contrato de terceirização de segurança. As métricas tradicionais, como disponibilidade e tempo de resposta, continuam válidas, mas não são suficientes. No contexto de segurança, surgem novas medidas como o nível de proteção garantido e o nível de atualização dos sistemas.

A decisão de terceirizar ou gerenciar segurança com recursos próprios depende de cada corporação. A terceirização é uma tendência, mas, dependendo de condições particulares, pode não ser o melhor caminho para todas as corporações. Para estabelecer critérios de comparação com uma abordagem de gestão com recursos próprios, é importante identificar as reais necessidades da organização relacionadas com segurança, avaliar a situação atual e delimitar o âmbito e as fronteiras de um potencial contrato de terceirização, determinando os recursos internos e ferramentas necessários para atingir o nível desejado de segurança.

Na tomada de decisão é fundamental a ponderação dos benefícios e dos riscos inerentes à terceirização. As decisões de terceirizar também devem levar em conta a análise do nível de desempenho e funcionalidades desejadas, capacidade atual de realizá-las com recursos próprios, nível de customização requerido, tendências de evolução no contexto tecnológico, infra-estrutura de segurança existente e custos associados, além da consideração da estratégia de terceirização da organização como um todo e sua tolerância ao risco.

A decisão pela terceirização da segurança também diz respeito a questões relativas à extensão de seu escopo. É consenso que nem todas as atividades envolvidas na gestão da segurança de uma corporação são terceirizáveis. Em particular, as atividades mais operacionais relacionadas com a administração e o monitoramento da infra-estrutura de segurança estão mais sujeitas à terceirização.

Se considerarmos a corporação a partir de uma perspectiva de fora para dentro, é mais comum que as corporações comecem pela terceirização dos elementos de segurança mais próximos da fronteira LAN/WAN de sua rede, como *firewall*, IDS e concentrador VPN. A evolução natural desse processo de terceirização da segurança se dá no sentido da LAN, dos *desktops* e dos servidores, abrangendo, por exemplo, soluções de antivírus, *anti-spam*, controle de acesso de usuários. É uma abordagem que permite que as corporações testem o conceito da terceirização da segurança de forma gradual, começando por elementos mais externos, minimizando os riscos de insucesso e ganhando confiança gradativamente, até alcançarem a terceirização completa da infra-estrutura de segurança.

Como reflexo da criticidade da segurança da informação, o critério que possui peso significativo na seleção de um provedor de serviços de segurança gerenciada é o fator da confiança, da capacidade, de sua reputação, e de seu reconhecimento como prestador de serviços de excelência. O critério de seleção baseado em custo é importante, mas passa a figurar como segundo critério de decisão quando o assunto é segurança. Em vez de minimizar riscos com a contratação de um terceiro que monitore e gerencie os ativos de segurança, a escolha de um provedor que não seja confiável e com competência duvidosa pode aumentar os riscos inerentes à segurança.

Considerações finais

Contemporaneamente, segurança vem se tornando uma das prioridades mais relevantes para as corporações. Segurança passou a ser considerada um problema de negócios, um requisito essencial para competir numa economia globalizada e para atingir resultados sustentáveis no longo prazo.

A crescente utilização de tecnologia como viabilizador dos processos de negócio cria vantagens competitivas, expandindo, continuamente, as fronteiras da segurança. Crescentes vulnerabilidades dos sistemas e tecnologias introduzidas no suporte aos negócios e crescentes ameaças com elevado grau de sofisticação expõem a corporação a novos riscos a cada dia.

Nesse cenário, a abordagem tradicional de gestão da segurança, com foco apenas na utilização de ferramentas tecnológicas, torna-se inadequada. A segurança situa-se num contexto organizacional e operacional mais amplo e, portanto, não pode ser gerenciada como uma disciplina estanque. Faz-se necessária uma abordagem de gestão holística, levando em conta processos, pessoas e ferramentas com o objetivo de identificar, quantificar e minimizar os riscos ao negócio. A terceirização surge, assim, como uma das possíveis formas de obter uma gestão de segurança mais efetiva e proativa.


$342,00
$230,00
35,8%
a,B,c
%
$

Segurança da Informação

Um diferencial determinante na competitividade das corporações

Texto
Marcio Zapater
Rodrigo Suzuki

Colaboração
Alex Paulino
Luiz Faro
Yassuki Takano

Coordenação
Danilo Sella

Supervisão
Renata Randi
Jorge Leonel

Projeto gráfico
Art Urb

Ilustrações
Rubens Lima
Mauro Nakata

Revisão
Escrita

Promon
Business & Technology Review

Av. Pres. Juscelino Kubitschek, 1830
04543-900 São Paulo SP

Praia do Flamengo, 154
22210-906 Rio de Janeiro RJ

Brasil

www.promon.com.br