Soluções

Antivírus

Os vírus acabaram por formar uma grande indústria de antivírus.
Todos os vírus agem de forma semelhante. Existem dois métodos básicos usados para combater vírus. O primeiro consiste em manter nos antivírus uma base de dados onde ficam registradas todas as assinaturas (parte do vírus que o caracteriza) de vírus conhecidos. Daí a importância de manter seu antivírus atualizado, pois a cada dia surgem centenas de novos vírus. Assim, quando scaneamos o sistema, na verdade o que estamos fazendo é comparar cada arquivo nosso com a assinatura dos vírus registrados.
A segunda forma de proteção é conhecida como inoculação, que nada mais é que a criação de um banco de dados contendo as principais informações (tamanho, data de criação e data da última alteração) sobre os arquivos inoculados. Assim, cada vez que scaneamos o sistema o programa antivírus compara as informações do banco de dados criado com as que estão no disco. Se houver alguma diferença é emitido um alerta. Mas note que não é qualquer arquivo que deve ser inoculado, uma vez que arquivos de dados sempre são alterados. Os arquivos executáveis, DLLs e arquivos de sistema são exemplos de arquivos que devem ser inoculados, pois são as principais vítimas de vírus e não mudam seu conteúdo com frequência.

Algumas medidas de segurança

Nenhuma empresa está livre de ataques de vírus. Mas existem algumas medidas que ao menos podem diminuir o risco de contaminação. Em primeiro lugar é muito importante que haja uma conscientização por parte dos funcionários sobre as normas de segurança. Este é o primeiro passo para evitar problemas futuros.
Nada adianta uma equipe super treinada em segurança se os funcionários insistirem em baixar arquivos de origem duvidosa da rede externa, ou inserirem discos inseguros nos micros. Um dos pontos mais importantes do processo de conscientização dos funcionários é a questão do e-mail, pois este é o principal “trampolim” dos vírus atualmente.
Algumas medidas simples podem evitar muita dor de cabeça futura, tais como:
. Não abrir e-mails de pessoas desconhecidas.
. Não abrir arquivos executáveis anexados a e-mails, mesmo que venham de pessoas conhecidas.
. Não abrir documentos do Office contendo macros, se abrir, desabilitar as macros.
. Não baixar programas da Internet.
. Apesar de tudo, o ideal é ter uma equipe preparada para agir em caso de contaminação. Esta equipe deve se manter atualizada e não só tratar de contaminações, mas também da segurança do site em geral. Algumas atribuições básicas de uma equipe de segurança são:
. Manter o antivírus sempre atualizado.
. Fazer backups periódicos.
. Configurar os clientes de e-mail para não interpretarem HTML ou qualquer script.
. Configurar o Office para não executar macros sem permissão.
. Atualizar o Office periodicamente (devido a possíveis falhas que podem ser exploradas).

Segurança da Informação

A segurança da informação gera sempre muitas dúvidas nas pessoas, que vão desde as mais básicas, como usar ou não o internet banking, até as mais complexas, relacionadas a fraudes eletrônicas, como e-mails falsos enviados em nome dos bancos aos correntistas, clonagem de cartões de crédito e até o chamado redirecionamento de DNS. A maior parte dos problemas de segurança são causados por pessoas que tentam obter algum benefício ou

Para uma empresa que deseja implementar a segurança da informação com sucesso, ela deve seguir os passos: divulgar a cultura de segurança, garantir o desenvolvimento do projeto e após o término, sempre monitorar.

Conceito de segurança

A segurança, de uma forma simples, é a proteção necessária "das coisas" que possuem valor para a empresa, ou mesmo, uma pessoa, e na prática é controle do risco, ou seja, controlar o risco existente. Estas "coisas", podemos entender por informação, que é todo e qualquer conteúdo.
Não podemos eliminar os riscos e a segurança deve garantir os ativos.

Informações

Qualquer tipo de dado são informações e podem ser restritas ou uso público, mas serão sempre informações e sempre teremos o risco sobre elas.
Podemos ter 3 categorias de classificação, informação confidencial; informação de uso interno ou informação pública.

CIA
De Confidentiality, Integrity and Availability, traduzindo, Confidencialidade, Integridade e Disponibilidade.
Representa as principais propriedades que, atualmente, orientam a análise, o planejamento e a implementação da segurança das informações que se deseja proteger, resumindo, seriam os princípios básicos da segurança da informação.

Confidencialidade
Divulgação não autorizada. Limitando o acesso a informação somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação.

Integridade
Protegida contra modificações não autorizadas, devendo garantir que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).

Disponibilidade
O sistema deve estar disponível quando da sua necessidade, por aqueles usuários autorizados pelo proprietário da informação.

SGSI

Um Sistema de Gestão da Segurança da Informação-SGSI é um processo estratégico para a empresa, devendo estar sempre ligado ao negócio da mesma. Para sua implantação, devemos nos perguntar, proteger o que ? De quem ?

Depois de identificado o potencial de ataque, devemos decidir o nível de segurança a estabelecer para uma informação (rede, sistema ou recursos físicos e lógicos). No nível de segurança devem ser quantificados os custos associados aos ataques e os associados à implementação de mecanismos de proteção para minimizar a probabilidade de ocorrência de um ataque.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.
Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre

essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira). A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.
Existem duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido).

Políticas

Para a elaboração das diversas políticas, deve-se levar em conta principalmente:

- Riscos associados à falta de segurança;
- Benefícios;
- Custos de implementação dos mecanismos.

Aqui veremos as Políticas:
. de Uso de Recursos
. de Senhas
. de Back-up
. de Continuidade

Política de Uso de Recursos

Uma política de uso dos recursos de informática, é um documento que regimenta o uso e atribui direitos e responsabilidades aos funcionários que usam os recursos computacionais de uma empresa. Vale lembrar que a mesma política pode ser aplicada para terceiros, mas lembrando que neste caso as regras devem ser estabelecidas junto a empresa terceirizadora e não junto ao funcionário terceirizado para que não venha a caracterizar um vínculo empregatício.

É do conhecimento de todos que por melhor que tenhamos estruturado uma rede, ainda temos limitações. Também é do conhecimento de todos que o ambiente computacional não é uma "zona livre" onde tudo é possível e permitido. O bom uso dos recursos de processamento e de tráfego de uma empresa preserva o principal ativo nos tempos modernos: "A Informação".

Nesta abordagem, uma política de segurança deve preservar os três atributos de segurança da informação:

. Confidencialidade
. Integridade
. Disponibilidade

Como desenvolver

- elabore a política de segurança com apoio de todos da empresa, iniciando pela alta administração. Sem este apoio seu projeto não terá efeito;
- faça uma análise de risco para determinar onde se exige uma maior atenção para as ameaças e vulnerabilidades. Existem ferramentas gratuitas que podem lhe ajudar neste processo (Ex: MSAT e MBSA da Microsoft). Esta etapa ajuda a definir as prioridades e o planejamento dos investimentos neste processo;
- pesquise como os funcionários usam a rede e a internet usando ferramentas de varredura;
- planeje os propósitos e serviços do sistema com o foco no NEGÓCIO da empresa e não na tecnologia que os suportam;

- informe todas as áreas sobre o desenvolvimento da política e convide-os a participar. As áreas de Recursos Humanos e a área Jurídica de sua empresa precisam acompanhar todo o desenvolvimento, assim como o maior número de pessoas da alta administração (Presidente, Vice-Presidentes e diretores) ou ter representantes nomeados pelos mesmos neste processo com adequado grau de representatividade. Lembre-se que apenas "Corpo Presente" não resolve.

Após o desenvolvimento

- divulgue a política de segurança para todos os funcionários independente dos mesmos terem ou não acesso aos sistemas;
- estabeleça um processo de integração onde todos os novos funcionários recebam um treinamento a respeito da segurança da informação;
- faça palestras periódicas para todos os funcionários com consultores externos especializados, tenha uma cartilha de segurança com o resumo dos principais pontos de sua política ou mesmo implemente um ScrenSaver que apresente dicas de Segurança da Informação;
- revise sua rede em busca de alterações que possam invalidar a regimentação de sua política de segurança ou que tenham sido feitas posteriormente a análise de risco, comprometendo a rede;
- faça buscas e remoção periódicas de documentos que contenham informações que caracterizem sua rede e que estejam disponíveis nos servidores (Ex. tabelas de roteamento, lista de nomes de servidores, diagramas e etc)

Bom, agora vamos ao exemplo da estrutura de um documento que regimenta o Uso dos Recursos de Informática:

Escopo:

Na condução de seus negócios, a Empresa zela pela proteção de seu patrimônio, inclusive intelectual, e também pelo patrimônio de seus parceiros, sejam eles fornecedores, clientes ou a própria sociedade.
É entendimento da Empresa que a proteção de seu patrimônio é parte integrante da responsabilidade de cada um de seus associados e colaboradores, na medida em que todos devem agir com lealdade e zelo profissionais, a quem cabe conhecer as regras e limites legais e organizacionais.
Em decorrência do exposto acima, as seguintes regras regulam a proteção ao acervo intelectual e o uso de recursos e sistemas de informática, sendo aplicáveis aos FUNCIONÁRIOS que venham a utilizar equipamentos ou ter acesso a sistemas e informações, direta ou indiretamente.

Hardware

Os equipamentos fornecidos pela Empresa são de sua propriedade ou de sua posse, cabendo-lhe, nesse caso, responsabilidade sobre o uso regular que é dado aos mesmos.
Nesse sentido, os equipamentos fornecidos pela Empresa somente podem ser utilizados por quem detenha a devida autorização formal para tanto.

Software

Nos equipamentos utilizados pela Empresa somente podem estar instalados e em funcionamento sistemas devidamente autorizados e testados previamente pela área de Informática.
Esses sistemas são de propriedade da Empresa ou de terceiros, sendo a Empresa licenciada e, portanto, responsável pelo correto uso dos mesmos.

Regras Gerais:

- Nenhum software pode ser instalado ou transferido entre equipamentos sem a autorização prévia e formal da Empresa, através da área de Informática, sendo que essa regra vale também para downloads da Internet, independentemente de serem licenças grátis (freeware, shareware, demos, trials, etc).

- A cópia de software, exceto quando devidamente autorizada previamente pela Empresa e nos restritos limites das eventuais licenças, É VEDADA POR CONFIGURAR CRIME.

- A instalação ou uso de software que não seja de propriedade da Empresa, ou que não esteja a ela licenciado, requer a prévia autorização por parte da área de Informática e testes preliminares de sua atuação e impactos no sistema vigente.

- O uso de software pessoais somente pode ser permitido mediante autorização prévia, com a comprovação da propriedade da devida licença e também considerados os impactos que este software possa causar nos sistemas da Empresa.

Acervo da Informação

Pertencem, a título exclusivo de propriedade**,** os direitos sobre:

- Conhecimentos técnicos aplicados ou aplicáveis para solucionar problemas, documentos escritos, desenhos, plantas, arquivos magnéticos e/ou de informática, manuais, relatórios, etc, aplicados a:
    - novos produtos;
    - novas composições e combinações;
    - novas aplicações de composições conhecidas;
    - métodos e processos;
    - configuração e otimizações de parâmetros;
    - equipamentos, softwares ou metodologias para avaliar parâmetros técnicos e controlar a qualidade;
- Softwares desenvolvidos para e/ou dedicados exclusivamente à Empresa;
- Desenhos ornamentais, desenhos industriais e modelos de utilidade;
- Palavras, slogans, sinais ou marcas;
- Obras e elaborações de natureza artística ou editorial;
- Sistemas de organização e administração;

Sigilo

Todo e qualquer acesso a informações e/ou dados, em todo tipo de forma ou suporte conhecido, bem como os métodos, critérios e técnicas relacionados às atividades desenvolvidas pela Empresa e assim como às suas relações comerciais mantidas com terceiros, configuram segredos, seja industriais, comerciais ou de negócios.
É de conhecimento e dever do Funcionário:

- Estar ciente de que é vedada a divulgação ou a exploração, a qualquer tempo ou título, exceto mediante a prévia autorização escrita da Empresa , dessas informações e/ou conhecimentos ou outros que compõem a propriedade intelectual da empresa e que o uso indevido ou não autorizado pode redundar em prejuízos bem como caracterizar eventuais crimes contra a propriedade alheia ou de concorrência desleal.
- Estar ciente de que o acesso a essas informações e/ou conhecimentos ou outros que compõem a propriedade intelectual da Empresa somente se dá em virtude das funções desempenhadas.
- Reconhece que não irá revelar a terceiros, sem a autorização prévia e escrita da Empresa , qualquer parte do acervo de informações, bem como não irá se utilizar de qualquer parte do mesmo, exceto para o desempenho de suas funções.

Acesso e uso de sistemas informatizados

Todos devem estar cientes de que o uso dos sistemas deve ser feito de modo a preservar os interesses e a boa imagem da Empresa, de seu pessoal e da comunidade, evitando-se o uso indevido, abusivo, não autorizado e ilícito dos mesmos, de maneira a evitar-se a intrusão ou acesso não autorizado de terceiros.

Todos devem estar cientes de que o uso dos sistemas não é totalmente livre de riscos, sendo que, sempre que julgar conveniente, a Empresa tomará todas as medidas necessárias para restringir ou eliminar ações que possam ser potencialmente arriscadas, dentre elas:

- o uso não autorizado de sistemas;
- o uso dos sistemas para fins não alinhados aos negócios;
- o uso dos sistemas para práticas que possam expor os mesmos ou a empresa a riscos – inclusive de sobrecarga de redes, indisponibilidade de informações internas ou externas e etc.;
- o uso dos sistemas para contatos que sejam ilegais ou contrários a princípios morais ou que afetem os seus interesses, os interesses de seu pessoal e da comunidade.

Controle de Acessos e Senhas:

- O Funcionário declara que irá usar somente sua senha de acesso, a qual lhe foi atribuída pela Empresa, quando tiver acesso aos sistemas da empresa ou outros sistemas delegados ou licenciados para o exercício de suas funções.
- O Funcionário se obriga a se desconectar dos sistemas sempre que completar suas atividades ou quando tiver que se ausentar do local a qualquer título.
- O Funcionário se obriga a não divulgar sua senha de acesso, ou permitir que se tenha acesso a ela, reconhecendo-a como pessoal e intransferível. Caberá ao Funcionário toda e qualquer responsabilidade sobre as ações decorrentes da não observância desta regra.
- O Funcionário se obriga a não tentar conectar-se a sistemas ou buscar acesso a informações para as quais não lhe tenham sido dadas senhas ou nível de autoridade de acesso.
- O Funcionário reconhece que, exemplificativamente, serão considerados Usos não Aceitáveis as práticas apontadas no referido tópico desta Política.

Princípios e regras para o uso pessoal dos recursos disponibilizados:

O Funcionário reconhece que o uso pessoal de recursos de informática será sempre limitado, ocasional e em estrita observância à lei e às normas organizacionais e que isso implica:

- em princípio, tudo o que esteja em seus sistemas e arquivos, sob qualquer forma, pode ser ou tornar a ser propriedade da Empresa , podendo esta, acessar, apagar e/ou reproduzir os mesmos sem prévio aviso ou autorizações;
- o uso deve ser razoável, seja quanto à natureza, escopo e conteúdo;
- o uso deve levar em consideração os valores, a imagem e as posições da Empresa , e será de forma a não impactar negativamente a mesma, prejudicar o andamento dos trabalhos e das obrigações profissionais, de outros colaboradores, bem como não resultar, a juízo da Empresa, no consumo de recursos (espaços de memória, tempo, banda de internet e etc) de forma inadequada e/ou não razoável;
- que o uso será passível de acompanhamento direto ou indireto, sem aviso prévio, por parte da Empresa, por pessoal devidamente autorizado e com adequado nível organizacional, no exercício de suas funções dentro da Empresa, para a gestão e manutenção do ambiente corporativo.

Uso não aceitável

- Violação intencional da segurança do sistema de computação;
- Uso não autorizado de contas e códigos de acesso em computadores;
- Baixa (download) não autorizada de programas ou aplicativos (independente do tipo da licença), da Internet ou demais redes;
- Uso intencional das facilidades computacionais que consumam recursos desproporcionais ou injustificáveis, prejudicando as atividades normais da Empresa ou gerando indisponibilidade de informações ou serviços;
- Verificação ou acesso não autorizado a arquivos ou informações que digam respeito a terceiros;
- Envio, recuperação, acesso, exibição, armazenamento, impressão ou disseminação de materiais ou informações fraudulentas, coercitivas, ameaçadoras, ilícitas, racistas, de conotação sexual ou obscenas, intimidatórias, difamatórias ou de qualquer maneira em desacordo com uma conduta profissional;
- Qualquer tipo de comunicação eletrônica que possa vir a prejudicar a imagem da Empresa ou terceiros ou expor a empresa a ações de responsabilidade;
- Baixa ou utilização de ferramentas invasivas (Hacker / Cracker / Snnifers / etc.);

- Disseminação, armazenamento ou utilização de programas maliciosos (Vírus/Worms/etc.) e códigos prejudiciais, de maneira deliberada;
- Destruição ou danos intencionais a equipamentos, software ou dados que pertençam à Empresa ou a outros colaboradores;
- Interrupção intencional ou monitoração não autorizada de comunicações eletrônicas;
- Comunicação eletrônica sem identificação clara da origem verdadeira ou do remetente da mensagem;
- Uso de recursos da Empresa para conduzir negócios estranhos à mesma; realização de atividades para fins de ganhos pessoais, propaganda pessoal, angariar ou promover causas religiosas ou políticas; ou qualquer outra atividade que a Empresa entenda que não esteja dentro dos interesses da empresa ou previamente aprovadas e liberadas pelos gestores competentes;
- Transgressão de direitos autorais, marcas registradas ou outras propriedades intelectuais;
- Transgressão de acordos de licença de software;
- Encaminhamento automático de e-mails, a partir de contas do Correio Eletrônico da Empresa, para contas particulares.

Considerações Finais

Qualquer uso dos recursos da Empresa que caracterize transgressão desta Política ou qualquer política corporativa ou outras diretivas, será tratado com seriedade e poderá resultar em medidas disciplinares, inclusive demissão ou interrupção de outras formas de contratação.
Atos ilícitos envolvendo os recursos da Empresa também estão sujeitos a ação penal. As pessoas envolvidas no uso não aceitável de recursos de computação, de acordo com a legislação vigente, serão responsabilizadas civil e criminalmente por quaisquer danos que resultem de tais atos.

Política de Senhas

Entre as políticas existentes e utilizadas pelas empresas, a do gerenciamento de senha é a mais confusa, pois temos colaboradores (funcionários) que têm dificuldade em memorizar as senhas, além do hábito, já comum, de anotar as senhas em quaisquer lugares. Bem, para resolver isso, devemos ter em mente de sempre estar conscientizando os usuários sobre a segurança, fazendo a difusão da(s) política(s). Continuando...
Primeiramente, vamos entender quando utilizar a Política de Senhas, com este pequeno e simples exemplo. Digamos que eu tenha um datacenter de hospedagens de sites e neste datacenter eu tenha 6 funcionários. Este datacenter fornece serviços de hospedagens de sites e e-mails para empresas, bom, acredito que tenha entendido o que faz esta empresa, pois temos muitas por aí que fazem isso. Para os 6 funcionários, ou melhor, para as contas existentes dos funcionários assim como as contas de administradores dos sistemas, devemos ter uma Política de Senhas, mas não posso aplicar esta política para meus clientes, que são as empresas que hospedam seus sites comigo. Quem deve aplicar uma Política de Senhas para suas contas, são os próprios clientes, ou seja, cada um deverá definir como fazer com o gerenciamento das senhas.

Agora que entendemos quando se aplicar a Política, vamos ver como podemos fazer. Para que possamos ter um bom e seguro gerenciamento de senhas, podemos seguir as seguintes regras:
. Senhas com data para expiração, por exemplo, 30 dias. Com isso o usuário é obrigado a mudar sua senha. a cada 30 dias. Para as contas de administrador, é interessante colocar uma expiração de 15 dias.
. Proibir o uso de senhas comuns, como por exemplo, quaisquer datas, sequência de números, nomes, cores, etc.
. Proibir senhas já utilizadas anteriormente. Eu particularmente acho muito chato esta regra, mas é muito boa.
. Definir que a composição das senhas deverá ter caracteres numéricos e letras, por exemplo, “marco1”.
. Definir que a quantidade das senhas deverá ter um mínimo de caracteres, por exemplo, 9 caracteres.
. Definir um conjunto de palavras ou códigos que não podem ser utilizadas como senhas. Existem base de dados já prontas na Internet, onde é possível usar parte dela, assim como implementá-la, mas nunca usá-la no seu conteúdo default.
. Definir que informações particulares do usuário não poderão ser usadas. Por exemplo, meu nome sendo Marco e meu aniversário sendo em 15 de novembro, minhas senhas nunca poderão conter a palavra “marco” ou números como “15” e

“11” (mês de novembro).
. Para dificultar um pouco mais, podemos definir que as senhas deverão se iniciar por 3 letras, seguido por 2 números, seguido por uma letra e terminando com 4 números.

Para facilitar o gerenciamento da(s) regra(s) que implementou, você poderá usar aplicativos prontos ou até mesmo criar pequenos scripts que façam isso. No Linux/Unix, por exemplo, existem comandos que lhe ajudariam muito no gerenciamento de suas contas e senhas. Nos casos de softwares fechados em que se é necessário fazer o login do usuário, não será possível aplicar regras manualmente, ficando a disposição do software, ou seja, você só poderá usar a(s) regra(s) que o mesmo disponibiliza. Neste caso a melhor solução, e sempre, é a conscientização do usuário.
E finalmente, após chegar a um bom senso sobre as regras que irá usar no controle das senhas, você deverá escrever tudo isso que planejou, e o resultado será sua Política de Senhas. Lembrando que após terminar a Política, a mesma deverá ser divulgada para TODOS os usuários da empresa e, sempre a atualize e divulgue, fazendo um ciclo (verifique, atualize e divulgue).