Políticas de Segurança

Exemplo prático

Cenário (1)

- Empresa fictícia FazSoftware
  - Produz diversas aplicações para computadores pessoais
  - A sede da empresa é em Lisboa e tem uma delegação comercial em Leiria. A sede tem um acesso à Internet via ADSL de 2 Mbps e a delegação de 1 Mbps.
  - Existem mais de 200 colaboradores que trabalham fora das instalações da empresa, 50% são programadores
  - A empresa permite que os seus colaboradores trabalhem um dia por semana a partir de casa

Cenário (2)

- Empresa fictícia FazSoftware
  - Os vendedores passam a maior parte do tempo em viagens entre clientes e potenciais clientes. Por isso a FazSoftware implementou duas solução de acesso remoto:
    - Uma através de dial-in
    - Outra através da Internet via VPN's
  - A informação que entra através dos acessos remotos é considerada sensível
    - Os programadores trabalham sobre a última versão duma aplicação. Por isso a FazSoftware pode perder a sua vantagem competitiva se o código cair nas mãos da concorrência
    - A informação das vendas é altamente sensível, porque pode dar pistas aos concorrentes sobre os novos produtos.

Política de segurança

- Sumário
  - Abrangência
  - Gestão da infra-estrutura
  - Requisitos das passwords
  - Prevenção de vírus
  - Cópias de segurança
  - Acessos remotos
  - Acesso à Internet
  - Privacidade e registos
  - Informação adicional

Abrangência (1)

- Definir as políticas sobre o uso correcto da infra-estrutura informática. Esta representa um investimento com vista ao aumento da produtividade e da eficiência.
- São considerados componentes da infra-estrutura informática :
  - Toda a cablagem de suporte para dados e voz
  - Todos os equipamentos usados para o controlo do fluxo de dados e voz
  - Todo o software
  - Todos os dispositivos de entrada e saída como as impressoras, fax's e digitalizadores
  - Todos os componentes dos computadores, tais como: monitores, caixas, dispositivos de armazenamento, modems, placas de rede, memórias, teclados, ratos e fios

Abrangência (2)

- As acções não conformes com esta política de segurança serão alvo de acção disciplinar, sendo tratadas caso a caso
- A empresa reserva-se o direito de proceder a acções legais sempre que a lei vigente no país seja infringida ou quando ocorrerem prejuízos financeiros.

Gestão da infra-estrutura (1)

- Toda a manutenção, incluindo alterações de configuração nos computadores, deverão ser efectuadas apenas pelo pessoal da equipa técnica.
- Os colaboradores que não façam parte da equipa técnica não estão autorizados a efectuar qualquer modificação, mesmo aos computadores que lhe foram atribuídos pela empresa para desempenharem as suas funções

Gestão da infra-estrutura (2)

- As seguintes acções são consideradas modificações ao sistema:
  - Mudar a ligação de rede para outra tomada
  - Usar um dispositivo que permita efectuar o arranque de um sistema operativo alternativo (ex. disquetes ou cd-rom's)
  - Remover a tampa da caixa do computador
  - Instalar qualquer software, incluindo o software descarregado da Internet

Gestão da infra-estrutura (3)

- A gestão do hardware é restringida para:
  - evitar que as garantias dos fabricantes não fiquem inadvertidamente inutilizadas
  - que as precauções de segurança não são contornadas
- A instalação de software é restringida para garantir que:
  - a empresa cumpre todos os requisitos legais respeitantes a licenças
  - existe suporte adequado, pela equipa técnica da empresa, a todo o software existente
  - não existem incompatibilidades de software

Requisitos das passwords (1)

- A cada utilizador será atribuído um username ao qual estará associada uma password.
- A password garante que apenas os utilizadores autorizados acedem aos recursos da rede.
- É da responsabilidade de cada utilizador garantir que a sua password permanece secreta

Requisitos das passwords (2)

- Regras:
  - As passwords têm de ter pelo menos 8 caracteres alfanuméricos
  - As passwords não podem consistir em palavras, ou variantes, do nome do utilizador, do username, do nome do servidor ou da empresa
  - Os utilizadores são obrigados a mudar de password de 60 em 60 dias. Caso isso não aconteça a conta do utilizador será bloqueada. Para reactivar a conta o superior do utilizador terá de efectuar um pedido à equipa técnica.

Requisitos das passwords (3)

- Regras:
  - Durante a autenticação o utilizador tem 3 tentativas para introduzir a password correctamente. Se todas falharem a conta será automaticamente bloqueada. Para reactivar a conta o superior do utilizador terá de efectuar um pedido à equipa técnica.
  - Todos os computadores da empresa devem ter um screen saver que é activado ao fim de 15 minutos de inactividade. Depois de activado o sistema deve pedir novamente a autenticação do utilizador antes de conceder acesso.

Requisitos das passwords (4)

- Regras:
  - Para os acessos remotos (por dial-in ou por VPN's) os utilizadores têm de um utilizar o token de segurança que lhes foi atribuído. Este irá gerar automaticamente uma password nova a cada 60 segundos.
  - As passwords são privadas e intransmissíveis. Espera-se que o colaborador não escreva a sua password num papel nem a partilhe com outras pessoas. A única excepção será quando tal for pedido pela equipa técnica na presença do seu superior directo.
  - As passwords de acesso remoto têm de ser diferentes das usadas internamente.

Requisitos das passwords (5)

- Regras:
  - A empresa reserva-se o direito de imputar responsabilidades por danos causados pelo facto do colaborador não preservar a confidencialidade da sua password, de acordo com as regras estabelecidas.
- Uma política de passwords forte visa garantir a segurança de todos os recursos

Prevenção de vírus

- Todos os recursos informáticos devem ser protegidos por software antivírus
- É da responsabilidade dos colaboradores verificarem que o antivírus não está desligado
- Se um colaborador receber um aviso do software antivírus deverá cessar imediatamente a sua actividade e contactar a equipa técnica.
- É da responsabilidade da equipa técnica fazer a actualização do software antivírus. Esta será efectuada através de um mecanismo automático.

Cópias de segurança

- Uma vez por semana a equipa técnica fará uma cópia de segurança dos documentos guardados no computador de cada colaborador
- Será atribuído um dia da semana a cada colaborador para ser efectuada a cópia de segurança.
- Só serão feitas cópias de segurança dos documentos que estiverem dentro da directoria:
  - c:\My Documments
- É da responsabilidade do colaborador garantir que todos os ficheiros importantes são guardados na referida directoria
- As aplicações devem estar configuradas, por omissão, para guardar os seus documentos na referida directoria

Acessos remotos (1)

- Existem apenas dois métodos de acesso remoto permitidos pela empresa: dial-in e VPN's
- A ligação de modems à linha telefónica, nos computadores atribuídos aos colaboradores, é expressamente proibida e poderá servir como despedimento com justa causa
- O acesso remoto é concedido consoantes as necessidades. Assim o colaborador que queira obter permissões de acesso remoto terá que fazer um pedido ao seu superior directo que terá de dar o seu parecer e reencaminhar o pedido para a equipa técnica

Acessos remotos (2)

- Para os acessos remotos serão dados aos colaboradores:
  - Um token de segurança
  - Uma lista com os números de telefone dos modems disponibilizados
  - O software apropriado para as ligações VPN através da internet
  - Um guia sobre o acesso remoto aos recursos da rede da empresa

Acessos remotos (3)

- A empresa não é responsável pelo suporte do sistema que o colaborador usará para efectuar o acesso remoto.
- O colaborador ao aceitar o software será responsável, no seu sistema, pelas actualizações necessárias para obter acesso remoto, nomeadamente:
  - Uma linha telefónica
  - Um modem
  - Um processador mais rápido
  - Memória adicional
  - Etc.

Acessos remotos (4)

- A empresa é responsável pelo suporte técnico apenas na rede interna e respectivo perímetro.
- A resolução de todos os problemas de ligação, fora do âmbito referido, são da responsabilidade do utilizador
- O colaborador terá de assinar um termo de responsabilidade onde se compromete a manter a confidencialidade dos dados de acesso remoto, incluído o software.
- A não verificação do ponto anterior poderá dar origem a um processo de despedimento com justa causa.

Acesso à Internet (1)

- Os recursos da empresa, incluindo os que são usados para o acesso à Internet, são para o uso decorrente das actividades laborais. Esta política visa a utilização correcta dos recursos da empresa e aplica-se de equitativamente a todos os colaboradores.
- Os superiores directos dos colaboradores podem autorizar excepções desde que cumpram os seguintes requisitos:
  - O uso pretendido seja ocasional

Acesso à Internet (2)

- (continuação)
  - Não interfira com as tarefas habituais do colaborador
  - Serve os interesses legítimos da empresa
  - Tem fins educativos dentro do âmbito das funções do colaborador
  - Não infrinja as leis nacionais
  - Não sobrecarregue a rede

Acesso à Internet (3)

- Navegar na Internet
  - É obrigatório o uso de um browser que permita as seguintes configurações/requisitos:
    - Não conter plugins adicionais, além da versão base
    - Desligar a execução de Java e Java Scripting
    - Desligar os a aceitação de cookies
  - Estes requisitos visam garantir que os colaboradores não executem, inadvertidamente, código malicioso.
  - O não cumprimento destes requisitos resultará na perca de privilégios de navegação na internet
  - A instalação de browser deverá ser efectuada apenas pela equipa técnica

Acesso à Internet (4)

- E-mails
  - A recepção e envio de e-mails está limitado a mensagens com um tamanho igual ou inferior a 10 MB
  - Sempre que for necessário efectuar transferências de ficheiros de tamanho superior deverá contactar a equipa técnica para usar o servidor de FTP
  - Todas as mensagens transmitidas para listas de e-mail devem conter a seguinte informação como parte integrante da mensagem:
    - As opiniões expressas nesta mensagem não reflectem a posição do meu empregador
  - A empresa reserva-se o direito de impedir a transmissão das mensagens que não estejam conforme o ponto anterior
  - Os recursos informáticos da empresa não podem ser usados para aceder a contas de e-mail pessoais baseadas em servidores na Internet

Privacidade e registos

- Todos os recursos informáticos são propriedade exclusiva da empresa, incluíndo: e-mails, ficheiros armazenados, transmissões de dados, etc
- A empresa reserva-se o direito de monitorizar e registar toda a actividade existente na rede informática
- O colaborador é responsável pela entrega de todas as suas passwords, ficheiros, ou outros recursos, se tal lhe for pedido pelo seu superior directo.

Informação adicional

- Todas as dúvidas ou omissões que existam relativamente a este documento devem ser colocadas ao superior directo do colaborador
- Os superiores directos dos colaboradores têm a responsabilidade de encaminhar as questões para o departamento mais apropriado da empresa

Bibliografia

- Este exemplo é uma adaptação da política de segurança existente no anexo B do livro de Chris Brenton “Mastering network security” da Sybex.