18 – Abril de 2000

Segurança: muito mais do que tecnologia

Contratar uma consultoria, um integrador ou um fornecedor que implemente uma solução isolada de software ou hardware, prometendo resolver todos os problemas de segurança eletrônica e garantir a integridade, confidencialidade e disponibilidade das informações. Parece uma boa idéia mas, na verdade, representa um erro cada vez mais comum no ambiente corporativo atual. Segurança não se faz com a simples aplicação de tecnologia. Este pensamento, no entanto, não está de todo errado se voltarmos no tempo e percebermos que o conceito de segurança eletrônica um dia não existiu. A vivência, o dinamismo dos negócios e a velocidade da evolução tecnológica nos levou a criar este conceito e a repensá-lo dia-à-dia.

A própria tecnologia talvez tenha sido o primeiro e único recurso disponível quando, depois de agregada ao negócio, começou-se a pensar em segurança. O firewall, que segmenta a rede interna da externa, protegendo-a, tem seu importante papel. Também os roteadores que apontam o caminho e bloqueiam pacotes mal intencionados e o Proxy, que se dedicava originalmente à melhoria da performance da rede e passou a incorporar funções de análise de tráfego.

Softwares de detecção de intrusos, que monitoram o tráfego da rede e permitem ações mais ágeis, cumprem bem o seu objetivo. A criptografia, com suas chaves, garante a integridade e confidencialidade dos dados que trafegam pelas malhas cada vez mais capilarizadas. Os antivírus também cumprem o que prometem, rastreando todo tipo de informação à procura de códigos de programas mal comportados. Mais recentemente, o firewall pessoal estende a ação dos tradicionais firewalls até as estações de trabalho, proporcionando controle e monitoramento na utilização dos recursos computacionais.

São muitas as soluções de segurança baseadas em tecnologia, mas no meio de todos esses bits e bytes, ainda existe um elemento que - apesar de estar sendo esquecido - sempre esteve presente, com um papel mais importante do que tudo o que foi dito: **o ser humano.**

O homem é a engrenagem motriz, a peça que faz a máquina corporativa funcionar. É o responsável por toda tecnologia que serve de infra-estrutura para os negócios. Ele é quem manipula os computadores, os programas e também as informações. E que toma as decisões depois da análise do *output* tecnológico. Portanto, ratificando a tendência evolutiva do conceito, posso afirmar que segurança corporativa é muito mais do que pura tecnologia. É a gestão inteligente de processos, pessoas e infra-estrutura tecnológica. A gestão inteligente da informação em todos os ambientes!

A nova "corrente da segurança" tem identificado um importante elo chamado Pessoas. Este elo não precisa de patches de correção ou de um upgrade, mas de uma Política de Segurança, Nivelamento em Segurança da Informação, Campanhas de Divulgação e Classificação de Informações. As pessoas precisam entender sua importância no cenário da

segurança corporativa e você – enquanto empresa – precisa garantir o seu comprometimento.
Eis um bom exemplo de Norma Geral de Chaves e Senhas que deve compor um Política de Segurança Corporativa, personalizada de acordo com a cultura da empresa:

Definições

- Entende-se como "usuário" a pessoa que utiliza os recursos tecnológicos para executar suas atividades corporativas.
- Entende-se o como "chave" a identificação do usuário no ambiente prestador de serviços, associada à uma senha.
- Entende-se como "senha" a seqüência de caracteres necessária para autenticar e validar o acesso do usuário, sendo utilizada à uma chave.
- Entende-se como "senha fraca" a seqüência previsível de caracteres em virtude de repetições, por ser associada a dados inteligíveis, ou ainda por ser formada por menos de 8 caracteres.

  Exemplos de senha fraca: 12345, Marcos e 260972
  Exemplo de senha forte: 4Ax$gr5S

Disposições Gerais

1. CHAVES E SENHAS

1.1. A senha do usuário será pessoal e intransferível, sendo este responsável por sua utilização.

1.2. É proibida a divulgação da senha. Em caso de suspeita da perda de sigilo, a senha deverá ser trocada imediatamente.

1.3. É proibido o compartilhamento de senha com outros usuários.

1.4. A chave do usuário deve ser a mesma em todos os ambientes e sistemas, permitindo assim, a sua identificação única.

1.5. Recomenda-se manter a mesma senha sincronizada nos diversos sistemas e ambientes a que o usuário tenha acesso.

1.6. Deverá ser evitada a adoção de senhas previsíveis, tais como: datas, nomes próprios, palavras do dicionário ou siglas comuns. Recomenda-se fazer uma combinação entre números e letras, o que pode ser aprimorado acrescentando-se caracteres especiais e letras em caixa alta e baixa.

1.7. A chave de acesso do usuário será definida de acordo com a cultura da empresa e os padrões abaixo:

1.7.1. Os usuários do Suporte terão duas chaves distintas: uma com direitos especiais para as tarefas de administração e outra como usuário comum para o seu uso cotidiano.

1.7.2. A chave de acesso do usuário será suspensa após 6 (seis) tentativas inválidas de conexão à rede corporativa e deverá ser registrada em log para auditoria. Somente poderá ser liberada com solicitação formal do gerente ou superior.

1.7.3. Cada usuário só terá direito a uma conexão simultânea por servidor de rede.

1.7.4. A regra de formação para a chave dos usuários será:

1.7.4.1. No caso de funcionário, os 2 (dois) primeiros caracteres representam o estado, os 2 (dois) seguintes representam o departamento e os 2 (três) últimos as iniciais do nome;

RJ= Rio de Janeiro

DM = Departamento de Marketing

MS = Marcos Sêmola

Exemplo: Chave RJDMMS

1.7.4.2. Caso existam combinações iguais de chave de funcionário, deverá se utilizar um outro sobrenome.

1.7.5. Em todos os ambientes o tamanho mínimo da senha será configurado para 8 (seis) caracteres e o usuário será forçado a trocar sua senha no primeiro acesso.

1.7.6. As senhas terão validade de até 60 (sessenta) dias, sendo que automaticamente o ambiente de rede solicitará a sua troca em seu vencimento.

1.7.7. Chaves de acesso não utilizadas no período de 45 (quarenta e cinco) dias serão bloqueadas automaticamente através do sistema operacional da rede.

1.7.8. A solicitação de acesso e o desbloqueio dos usuários da rede, deve ser formalizada através do sistema de solicitação de acesso.

1.8. Todos os usuários terão uma senha única para acesso a rede corporativa.

1.9. A senha não deverá ser anotada em hipótese alguma e sim memorizada.

1.10. Para acessos de emergência, toda a senha de alto nível compartilhada deve estar em um envelope selado acessível somente aos usuários autorizados pela gerência a utilizar a senha.

1.11. As senhas devem ser revogadas, as permissões de acesso removidas e os tokens de autenticação devolvidos imediatamente em caso de desligamento do funcionário.

Se sua empresa acompanha a evolução da tecnologia sem esquecer da segurança que garantirá a continuidade do seu negócio, não se limite a soluções pontuais que resolvem problemas isolados.

> *"A eficiência da Corrente da Segurança está diretamente relacionada ao nível de segurança do elo mais fraco."*

O negócio é uma máquina com processos, que por sua vez são geridos por pessoas e tecnologias. Portanto, é preciso pensar no todo e entender o papel de cada engrenagem, agindo sobre elas com equilíbrio, pois são os elos da sua corrente!

A resposta para estas questões está na retaguarda de segurança, na abrangente e customizada solução de segurança corporativa...Enterprise Security Planning.

Em tempo, cabe um agradecimento aos especialistas em segurança eletrônica Eduardo Poggi e Vítor Hugo pela contribuição literária que ratificou o conteúdo deste artigo.

Marcos Sêmola *é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Gerente de Produtos e Analista de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br