Você é o Dr. House da Segurança da Informação?*

Sinto muito! Como não implementar medidas de segurança da Informação.

Não é de hoje que discutimos com os alunos acerca de um novo modelo de gestão de SI, baseada no elemento central: Pessoas! Dentre todas as vulnerabilidades que se possa mapear em uma empresa, nenhuma atinge com tanta contundência os objetivos da segurança da informação (confidencialidade, integridade, disponibilidade) do que pessoas! Pessoas são o elo fraco de qualquer ativo informacional, e por mais que nos preocupemos com ameaças físicas e lógicas, se as humanas não tiverem a devida gestão, a probabilidade do risco é enorme.

Já dizia o velho lema de segurança da informação: "Não há patch que resista à burrice humana". E a reflexão começa a fazer sentido quando um belo dia você pergunta para a Gerente de Finanças de sua empresa onde ela salvou a planilha de pagamentos, e ela, assustada, lhe responde "Ah, está na minha máquina, no Excel!" Boom! A pessoa não tem sequer a noção de sistema de arquivos, hierarquia entre pastas e arquivos, imagine se ela não clicaria naquele "pishing" e-mail com erros de português para verificar "As últimas fotos da vítima do seqüestro" antes de ser assassinada. Você tem dúvida?

A solução é assistir, monitorar, implementar medidas de segurança, e surge uma nova discussão, como implementá-las sem causar a revolta dos membros do operacional e gerência intermediária? A discussão é longa eis que muitos profissionais de TI culpam os usuários "desobedientes" pela falha dos planos! Mas será que a culpa é dos usuários e demais colaboradores ?

O problema pode estar com você, profissional de Segurança da

Informação! Mesmo depois de muitos anos de existência, a área de SI ainda é considerada coisa para poucos do ponto de vista técnico. Ela seria algo como o "fronteira final" em termos de aprendizado. Para poder compreender a segurança de uma tecnologia, você precisava dominá-la totalmente. Por conta disso, ela sempre atraiu muitos profissionais de alta capacidade técnica. Quando a empresa se deu conta que precisava de alguém para cuidar do assunto, lembrou que havia um técnico trabalhando há anos na empresa. Contratar alguém no mercado seria caro. Além disso, como confiar algo tão crítico a um desconhecido? Logo, por que não promover o técnico a gestor ou coordenador de SI? O problema é que nem sempre esses profissionais têm um perfil exatamente adequado para a posição.

A Ti sempre foi conceituada como a profissão do "Eu". Jamais questione um projeto de outro técnico! O jogo de empurra-empurra na TI é presente até hoje: O técnico do servidor leva a senha root para casa, como se fosse DEUS, e não deixa a equipe implantar o ERP. A equipe de ERP diz que o problema na lentidão no sistema é por culpa do DBA. E o DBA? "Ah, o problema é do link, ligue para o 0800 da Telefonia…" Jogo de cobras, ninguém assume erros ou colabora! Este perfil deve mudar, pois a TI perdeu muito com isso! Durante anos o técnico de TI foi conhecido como o "Naufrago do CPD", um ser isolado dentro de uma caixa que matinha relações apenas com seu "Wilson", diga-se, seu computador. Resultado, quanto mais técnico e isolado, mais técnico e isolado será. Me respondam… Na empresa em que trabalham? O CIO tem formação em TI ? Ou foi "importado" da Administração, do Direito, etc…? É…preocupante não ?

Costumamos brincar que muitos profissionais de Tecnologia da Informação (TI) escolheram esta área justamente para não precisar lidar com pessoas. É um paradoxo curioso que eu chamaria de Complexo de House. Para quem não conhece, House é um seriado médico de grande sucesso, com um personagem

principal homônimo, que goza de uma incrível popularidade entre os profissionais de TI. Se nós pudéssemos resumir a personalidade de House, poderíamos dizer que: É um brilhante médico, mas que não gosta de pacientes! Fica fácil entender porque o seriado é amado pelos profissionais e Estudantes de TI. Assim como o Dr. House, na maioria da vezes, em maior ou menor grau, profissionais de TI não gostam de usuários.

Não existe nada mais perigoso que colocar alguém que não gosta de usuários para definir medidas de segurança. Se trabalhando em TI ele já foi responsável por bloquear até a troca do papel de parede das estações, imagine o que ele pode fazer em escala empresarial! Profissionais com esse perfil não costumam possuir sensibilidade para perceber o quanto é delicada e incômoda a mera existência de um departamento de segurança. Não observam o quanto o contexto é capaz de mudar o comportamento das pessoas que nele atuam.

Para elucidar, deve-se destacar um famoso estudo de sociologia feito na Alemanha na década de 70 em um presídio desativado. Voluntários foram chamados a fazer o papel de policiais e presidiários em uma espécie de brincadeira de "faz de conta". Os pesquisadores observaram que, independente do perfil, aqueles que se passavam por policiais desenvolviam uma tendência ao autoritarismo. Já os presidiários se dividiam entre os resignados (que fingiam cooperar, mas não aceitavam a situação) e os rebelados. O estudo é bastante famoso, foi transformado em documentário, e não pôde ser acabado, porque a influência que o ambiente exercia sobre os atores era tamanha que as coisas começaram a fugir do controle.

Nas organizações ocorre uma situação bastante similar. Alguém é promovido a "policial" e, a partir de então, passa a ser exorcizado (ou tratado com falsidade) pelos "presidiários" (se nunca mais te chamaram para um *happy hour* depois da sua promoção, você sabe bem do que eu estou falando). Numa tentativa de mostrar poder e exercer a sua autoridade, o profissional passa a entrar em embates e tomar medidas de

eficácia duvidosa ou de prioridade questionável. Ou seja, ao invés de trabalhar para azeitar uma relação que é inerentemente conflitante, trabalha no sentido oposto. Não é difícil imaginar o resultado disso. Alguém na empresa deverá tomar a decisão de demiti-lo, independente de sua capacidade profissional. O trabalho de um gestor de SI é servir como um agente de mudanças, é ser um facilitador no processo de implementação de medidas que de certo modo privam a liberdade dos colaboradores. É impossível fazer isso brigando com toda a empresa. Entre demitir todos os empregados e demitir o gestor de SI, não é difícil imaginar qual a melhor decisão a ser tomada.

Existe uma verdade que precisa ser aceita. Ninguém gosta de medidas de segurança, a não ser aqueles que estão na posição de defini-las e cobrá-las dos outros. Quando se está sujeito às medidas de segurança, todos a detestam. Porém, num belo dia, a área de segurança é "promovida", ganhando independência. Pode apostar que as primeiras medidas de segurança terão como objetivo atormentar a vida dos técnicos: restrição de uso das contas dos administradores, geração excessiva de *logs*, controle de mudanças, etc. Estoura o conflito: os técnicos alegam que os profissionais de segurança, agora que são independentes, sugerem controles que jamais recomendariam se fossem responsáveis por sua implementação. Aí é que reside toda a eficácia da separação. Medidas de segurança geram trabalho e desconforto e ninguém gera isso para si mesmo. Se assim o fizer, não estará recomendando aquilo que é necessário, e sim aquilo que dará menos trabalho.

Para alguns, essa sutilezas podem parecer óbvias, mas conhecemos profissionais com anos de experiência que ainda não se tocaram. Colocar um técnico com o perfil do Dr. House para escolher medidas de segurança é uma estupidez administrativa, pois esse tipo de profissional não trabalhará para diminuir essas arestas, e sim para acentuá-las, criando um porno de

discórdias e desavenças. Além disso, ele não possui uma das características básicas para amenizar os problemas que é a capacidade de dar o exemplo. É muito comum ver profissionais de segurança dando sermão nos usuários em campanhas de conscientização, recomendando uma série de procedimentos que eles mesmos não seguem. Se você questioná-los, ouvirá algo do tipo “eles não podem usar o MSN, ou ORKUT porque não sabem amenizar os riscos, mas eu sei”. Ridículo!

Essa postura até encontra embasamento técnico, mas não há nada mais ineficaz, além de arrogante, em termos de postura. Técnicos que não gostam de usuários costumam pensar que são seres superiores. Deuses com todos os poderes nas mãos. Podem criar e apagar fatos incriminadores a qualquer momento. Seguem um estereótipo muitas vezes atribuído a padres: “faça como eu digo, mas não como eu faço”. Quando o padre diz “vivam juntos para sempre” soa meio caricato, pois ele nunca casou com ninguém! Você jamais vai ter moral para pedir aos usuários para interromper o uso do MSN se você continuar usando a ferramenta todos dias.

E para a Cúpula estratégica aqui vai nosso recado. Você tem controle dos ativos informacionais de sua empresa? Confia no seu “Gestor de SI” ? Conhece as senhas, processos e técnicas adotados pelo mesmo ? Se ele sair amanhã, tudo continua? É, trilhas de auditoria de Gerência podem ajudar! Se algum dia você precisar ligar para seu Gerente para ter acesso a alguma informação na Empresa, saiba, você está nas mãos dele! Aliás, a TI é uma profissão de poder, e poder corrompe! Confiar piamente no seu técnico promovido à Gestor seria entender que Gerentes de TI seriam todos heróis incorruptíveis que em nenhum momento tomariam um café com um funcionário, onde poderíamos ler seus lábios dizendo “Sua batata assou, quero metade em troca de um delete!” Audite a Auditoria, mas não seja “Policial”!.

Se você conseguiu visualizar claramente o problema, ótimo! Faça uma auto-crítica e avalie seu comportamento dentro do seu

ambiente de trabalho. Você está mais para Dr. House ou para Dr. Wilson? O primeiro sem dúvida é mais brilhante, mas não é ético, e só não foi demitido porque tem o segundo para segurar a barra quando a coisa estoura de verdade. E se você pensar bem, eles têm muito mais semelhanças do que diferenças, o que significa que não é tão difícil assim ter uma postura correta e equilibrada, mesmo que você tenha algumas excentricidades. Lição do dia: Não são pessoas que devem se adaptar à TI, mas a TI que deve considerar pessoas na adoção de medidas de segurança da informação. Se você achar que é um "Policial", terá dois tipos de presidiários: Funcionários Rebelados e Funcionários Resignados. Então, prepare-se para o pior!

*** NOTAS:**

1) Artigo Derivado Segundo Licença Creative Commons: *Artigo Orignal de Anderson Ramos, "*Como não implementar medidas de segurança – Parte 1*", publicado em 07-02-2008 em* http://aramos.org/2008/02/como-nao-implementar-medidas-de-seguranca-parte-1/#more-133

2) Leia a Licença aplicável ao Artigo em Tela:
http://creativecommons.org/licenses/by-nc-sa/2.5/br/