MODULO
Technology for Risk Management

FUNDAÇÃO GETULIO VARGAS

MBA em
Gerência de Telecomunicações

TCC - Trabalho de Conclusão de Curso

Treinando macacos, educando pessoas

Roberto Cunha

Segurança da Informação se faz com tecnologia, processos e pessoas, e a formação destas exige mais que uma seqüência de treinamentos.
Porque você treina macacos. Pessoas, você educa.

Treinando macacos, educando pessoas

Roberto Cunha

Segurança da Informação se faz com tecnologia, processos e pessoas, e a formação destas exige mais que uma seqüência de treinamentos. Porque você treina macacos. Pessoas, você educa.

Coordenação

Acadêmica: André Valle e Raul Colcher

Administrativa: Bernardo Griner

Orientação do TCC: André Valle

Resumo

O uso intensivo de computadores pessoais como instrumento de trabalho causou um aumento significativo da preocupação com a Segurança da Informação. Para atingir níveis confiáveis de segurança, o foco de muitas empresas tem sido investir primariamente em tecnologia e processos, esquecendo-se dos recursos humanos que necessariamente trabalharão com estas tecnologias e farão funcionar os processos.

O aumento exponencial da quantidade de conhecimento a ser apreendido – com a contrapartida do aumento exponencial da ignorância –, o crescimento da infra-estrutura e da complexidade das redes de comunicação e do número de usuários aumenta a importância do fator humano como elemento vulnerável dentro da cadeia de recursos que forma a Segurança da Informação. Mais pessoas, com menos tempo, têm de entrar em contato com equipamentos e programas que funcionam sobre tecnologias que elas mal conhecem, sujeitas a ataques e ameaças que crescem não somente em número mas também em suas diferentes formas de apresentação.

Neste contexto as tecnologias e os processos são insuficientes para garantir a Segurança da Informação. E mais: o simples treinamento dos recursos humanos também se mostra ineficaz, frente à contínua desatualização dos conhecimentos ministrados. É necessário educar as pessoas, indo muito além de simplesmente treiná-las.

Índice

CAPÍTULOS

FIGURAS

Introdução

Nós não somos computadores, Sebastian, somos de carne e osso.

O replicante Roy, em **Blade Runner**
(O Caçador de Andróides), 1982

No dia 26 de abril de 1986, à 01:23:58 hora local, o quarto reator da usina de Chernobil, na Ucrânia, sofreu uma explosão de vapor, seguida de um incêndio e de uma série de explosões e, por fim, ocasionando um derretimento nuclear. O pior desastre nuclear da história mundial ocorreu nas instalações de uma usina que operava há mais de onze anos e que possuía uma série de dispositivos de segurança. Um experimento programado para aquela noite pedia o desligamento de vários destes dispositivos e os avisos dos poucos que restaram acionados foram ignorados pelos operadores tanto por falta de informação dos mesmos com relação a certos problemas dos reatores quanto por pressão para que o experimento se encerrasse naquela mesma madrugada. A execução de procedimentos irregulares e a comunicação ineficiente entre os escritórios de segurança e os operadores também contribuíram para compor um quadro em que o fator humano foi decisivo para uma catástrofe cujos efeitos persistem até hoje[1].

Em 25 de janeiro de 2003, 05:29 GMT, o worm[2] Sapphire-Slammer, aproveitando-se de uma vulnerabilidade conhecida presente em dois produtos da Microsoft, começou a se disseminar pela rede mundial de computadores dobrando o número de máquinas infectadas a cada 8,5 segundos. Em três minutos atingiu o seu pico de velocidade de varredura (55 milhões de varreduras por segundo). Em 10 minutos já tinha infectado 90 por cento de todos os hosts vulneráveis conectados à Web. Em 30 minutos, mais de 75.000 hosts já estavam infectados. Causou uma diminuição violenta na largura de banda disponível da Internet e na operação dos mais diversos provedores de serviços (com ataques de negação de serviço – DoS) com efeitos tão diversos como o cancelamento de vôos de linhas aéreas, interferência em eleições, falhas de caixas automáticos de bancos, cinco horas de inatividade de um sistema de monitoramento de segurança de uma usina nuclear em Ohio/EUA e relatos de que, entre as máquinas atingidas, estariam pelo menos 5 dos 13 servidores de nomes por onde passa todo o tráfego da Internet mundial[3]. Apesar da Microsoft já ter conhecimento de tais

[1] Wikepedia, verbete 'Acidente nuclear de Chernobil', disponível em http://pt.wikipedia.org/wiki/Acidente_nuclear_de_Chernobil
[2] termo em inglês comumente utilizado para descrever um "verme de computador"
[3] http://www.caida.org/publications/papers/2003/sapphire/sapphire.html e D1.4 "Recommendations for Next Generation Monitoring Systems", INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME, 2005

vulnerabilidades em seus produtos e de haver disponibilizado uma correção para tais falhas desde julho do ano anterior, muitos administradores de sistemas não instalaram o patch de segurança que teria evitado tal propagação. A própria Microsoft teve parte de seus computadores infectados pelas mesmas razões. A companhia admitiu que alguns de seus servidores não foram atualizados porque os administradores "não cuidaram do problema quando deveriam"[4].

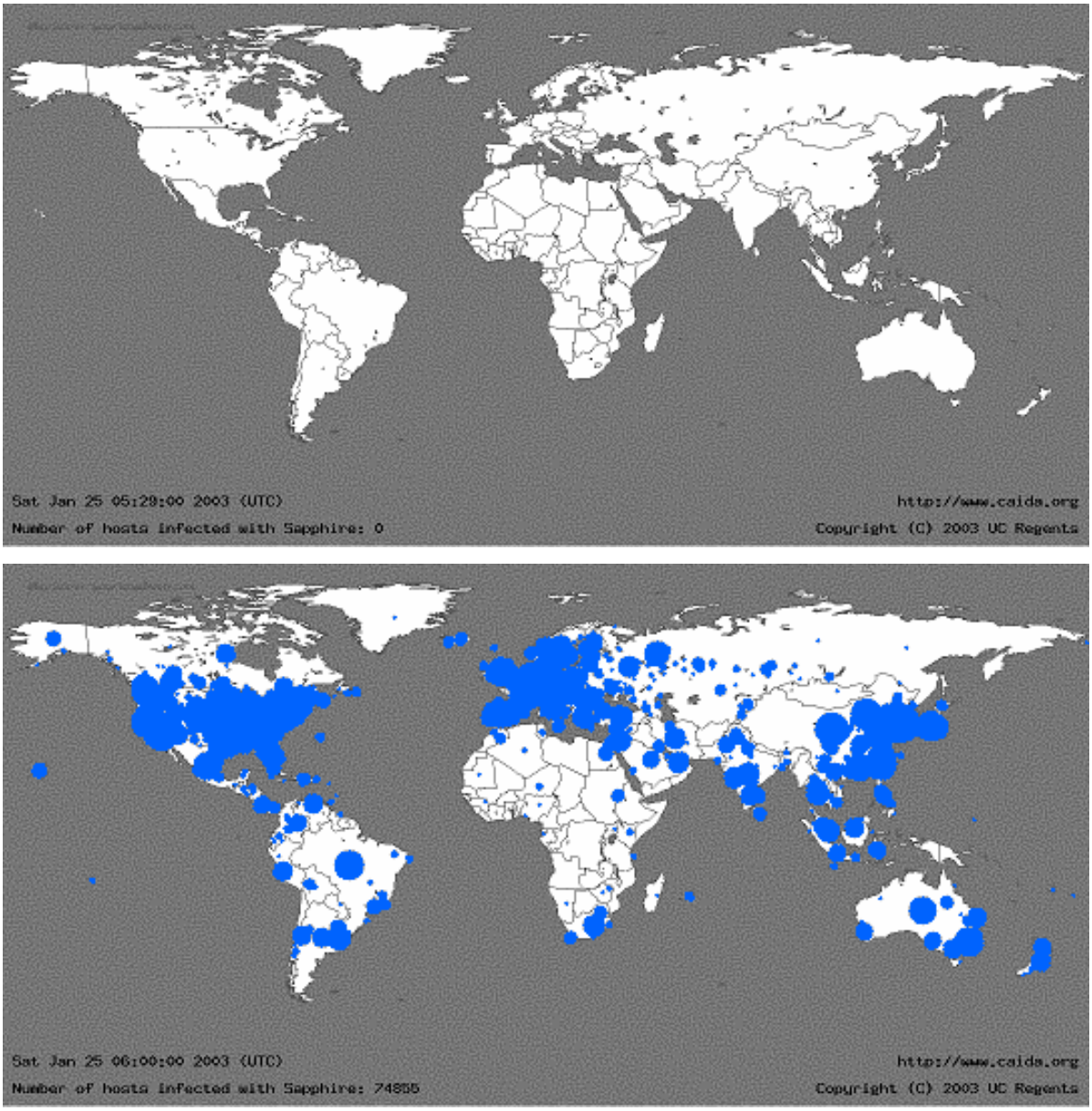

Figura 1 – Propagação do worm Sapphire-Slammer 30 minutos após ser lançado na Internet

[4] " Nem a própria Microsoft escapou do vírus SQL Slammer", disponível em http://www1.folha.uol.com.br/folha/informatica/ult124u12134.shtml

De acordo com um exemplo fornecido pela ISO – International Organization for Standardization e citado por Abby Christopher na Network World de maio de 2003, um ex-programador contratado por uma instituição financeira facilmente conseguiu passar pela segurança do edifício em que trabalhara porque os guardas simplesmente o reconheceram e acenaram para ele, permitindo a sua entrada. Uma vez dentro do edifício, fingindo ser um consultor realizando uma auditoria, interrogou um empregado que se sentiu na obrigação de fornecer a informação que estava sendo solicitada. Em seguida, conseguiu persuadir um outro empregado a verificar certa informação que ele, finalmente, utilizou para transferir 10,2 milhões de dólares do banco de sua ex-empresa para uma conta num banco suíço. Tal roubo só se tornou capaz com a cumplicidade involuntária de pelo menos três funcionários que, ignorando noções básicas de segurança, permitiram o acesso físico do criminoso ao prédio e forneceram acesso tanto à rede interna como aos bancos de dados[5].

O que estes três relatos têm em comum ?

Acredita-se comumente que a Segurança da Informação pode ser obtida com tecnologia correta e processos bem implementados. Esta crença de que somente tecnologia e processos seriam suficientes para tornar determinados ambientes e recursos seguros foi sistematicamente derrubada, nos três casos acima, quando *pessoas* desligaram controles, ignoraram avisos e deixaram de executar procedimentos e protocolos previamente estabelecidos.

Uma imagem recorrente é a de que segurança é uma cadeia formada por vários elos, tão forte quanto o seu elo mais fraco. Segurança da Informação, em particular, é uma cadeia que tem entre seus elos tecnologia, processos e pessoas. Os especialistas em Segurança da Informação são unânimes em apontar as pessoas como o elo mais fraco[6].

Por maiores que sejam os investimentos em tecnologia e processos, a corrente da segurança pode se romper com:

[5] " The Human Firewall", disponível em http://www.networkworld.com/research/2003/0526human.html
[6] http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39158023,00.htm, http://news.com.com/2100-7355_3-5278576.html, http://prescientconsulting.com/content/view/43/30/ e SCHNEIER, Bruce. Segurança.Com - Segredos e mentiras sobre a proteção na vida digital, Editora Campus, 2001, p. 255

- funcionários descontentes, que conhecem muito bem o que estão fazendo e se propõem a sabotar a empresa em que trabalham
- funcionários demitidos, que tiram proveito de seu conhecimento acerca da tecnologia e acerca dos processos internos da empresa para lesá-la
- funcionários mal treinados, que não conhecendo a tecnologia, nem os processos, nem os perigos a que eles estão expostos, põem em risco involuntariamente os ativos de sua empresa
- funcionários relapsos, que ainda que conheçam o que precisam saber para lidar com os vários aspectos da Segurança da Informação, de forma irresponsável negligenciam este conhecimento e derrubam, de dentro, todas as barreiras levantadas para proteção dos ativos da empresa

Os dois primeiros tipos de funcionários agem de forma intencional e criminosa. Os dois últimos, agem (ou se omitem) por ignorância/despreparo ou negligência. Com relação a estes últimos, pode-se dizer que lhes falta passar por um ou mais dos processos abaixo:

- conscientização: cuja falta se manifesta em comportamentos do tipo "não conheço, não faço" – ignorância passiva – ou "conheço e não faço" – não comprometimento –
- aquisição de conhecimentos básicos: cuja falta se manifesta com um "o que faço agora ?" frente as mais diversas situações, sejam rotineiras ou não
- treinamento: cuja falta se manifesta por perda de eficiência frente a situações rotineiras
- educação: cuja falta se manifesta pela ausência de uma atitude pró-ativa e alerta frente a situações não rotineiras

Por mais estranho e paradoxal que possa parecer, pouco é investido nas pessoas (relembrando, o elo mais fraco) quando se fala em Segurança da Informação[7]. Quando muito, aplicam-se recursos

[7] A pesar de 60% das quebras de segurança de informação em 2005 terem sido causadas por erros humanos, apenas 29% de 574 empresas entrevistadas ao redor do mundo disseram que o treinamento em segurança é uma obrigação para seus empregados, enquanto que 36% delas oferecem algum tipo de treinamento versando sobre conscientização de segurança (fonte: estudo da CompTIA - Computing Technology Industry Association citado em http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39158023,00.htm). Em 2005, o Human Firewall Security Awareness Index Survey detectou que 48% das companhias participantes da pesquisa jamais tinham oferecido treinamento de segurança formal para a sua força de trabalho. E das companhias que o tinham feito, somente 15% tinham oferecido tal treinamento nos seis meses anteriores.
(continuação da nota de rodapé)

somente em treinamentos os mais variados, como se só a implementação deste processo fosse suficiente para capacitar os recursos humanos nas empresas.

Os americanos têm uma expressão interessante a este respeito: "*You train monkey, you educate people*" ("você treina macacos; pessoas, você educa"). Educação, como veremos, é o ápice de um processo contínuo que se inicia com a conscientização, passa pela aquisição de conhecimentos básicos, fortalece-se com o treinamento até formar (educar) indivíduos preparados a lidar com situações novas, não previstas em sala de aula.

Para preservar os diversos ativos informáticos das empresas, devemos primeiramente entender as peculiaridades da Segurança de Informação e o papel do fator humano dentro dela. Quando percebermos que tecnologias e processos não são suficientes e que eles podem falhar em garantir tal Segurança, compreenderemos que temos de investir para ter pessoas melhor preparadas para compor a primeira (ou por vezes, a última) linha de defesa.

Educando pessoas (e não treinando macacos) é que ajudamos a construir empresas mais seguras.

(http://news.com.com/2100-7355_3-5278576.html).

Admirável (e alucinantemente rápido) mundo novo

Dr. Walter Gibbs: Ha, ha. Você tinha de esperar alguma estática. Afinal, computadores são apenas máquinas, eles não podem pensar.

Alan Bradley: Alguns programas logo estarão pensando.

Dr. Walter Gibbs: Isto não seria demais ? Computadores e programas começando a pensar e as pessoas parando.

Diálogo em **Tron**,
(Uma Odisséia Eletrônica), 1982

No início dos anos 80 cartas eram datilografadas, memorandos escritos a mão em blocos padronizados, apresentações eram feitas em flip-charts, transparências coloridas só eram possíveis com a colagem de papel celofane de diversas cores, planilhas eram feitas em papel quadriculado, pesquisas bibliográficas eram feitas consultando-se fichas de papel em armários de aço, que remetiam a índices remissivos no final de livros etc etc etc. Menos de uma geração depois, não se encontra uma atividade profissional, por mais corriqueira que seja, que não faça uso da computação: não somente engenheiros, técnicos, programadores e administradores de sistemas mas também secretárias, professores, palestrantes, caixas de banco e de supermercado, frentistas de posto de gasolina, bibliotecárias, operadores de equipamentos médicos, operadores de telemarketing, balconistas, farmacêuticos, leitores de consumo de água e eletricidade etc, todos eles dependentes da computação em menos de uma geração.

Qual seria a capacitação desta força de trabalho para ter acesso a equipamentos informatizados? Tomando-se por base somente o contexto brasileiro, o censo do IBGE 2000 apontou para um índice de analfabetismo de apenas 13,6 % entre jovens e adultos acima de 15 anos[8]. O Indicador de Alfabetismo Funcional (INAF) mostra, entretanto, que somente 26% da população adulta tem domínio pleno das habilidades de leitura e escrita e apenas 23 % tem nível pleno de alfabetismo matemático[9]. É esta população que foi imersa, em menos de uma geração, num novo mundo de comunicação e interação digital.

[8] http://www.ibge.gov.br/home/presidencia/noticias/noticia_impressao.php?id_noticia=288
[9] http://www.ipm.org.br/an_ind.php

Estima-se que 2 milhões de brasileiros comprarão seu primeiro computador no ano de 2006. Parte de um processo de inclusão digital, o barateamento dos equipamentos de informática e do software básico que normalmente os acompanha não encontra uma contrapartida investimento em treinamento e educação necessários à operação de tais recursos. E, quando ocorrem, se limitam a noções de "Windows, Word, Excel, Powerpoint e Internet", passando ao largo de noções de segurança. Basta dizer que não há nestes "pacotes" a necessária orientação sobre antivírus, firewall, anti-spyware/adware etc.

Não bastasse a ausência de treinamento e educação básicos, o próprio corpo de conhecimento a administrar é exponencialmente crescente.

Richard Saul Wurman lembra que *"uma edição do 'The New York Times' em um dia da semana contém mais informação do que comum dos mortais poderia receber durante toda a vida na Inglaterra do século XVII"*[10].

Outra forma de se encarar este problema é a célebre Lei de Moore. Entre as décadas de 60 e 70 Gordon Moore, um dos fundadores da Intel, enunciou que a capacidade de processamento dos computadores dobraria a cada 18 meses ao mesmo tempo que seus custos se manteriam constantes.

Figura 2 – Crescimento do número de transistores para processadores Intel e Lei de Moore
(fonte: Wikipedia, verbete "Lei de Moore", disponível em http://pt.wikipedia.org/wiki/Lei_De_Moore*)*

[10] WURMAN, Richard Saul. Ansiedade de informação - Como transformar informação em compreensão. São Paulo: Cultura, 1991, p. 36

Confirmada pela prática (vide figura 2), o que se tem é um aumento exponencial na capacidade de computação levando consigo, a reboque, a capacidade de armazenamento e, com ela, a quantidade de informações.

Ao mesmo tempo, a produção de informação e de conhecimento em geral dobra com uma velocidade espantosa. Dependendo da fonte, somos informados de que o conhecimento dobra de 5 a 10 anos, ou mesmo de 2 a 4 anos. Independentemente dos números, é mais do que óbvio que a quantidade de informação cresce de forma assustadora em todos os tipos de mídia (livros, revistas, jornais, rádio, televisão, Internet, TV por assinatura, CD, DVD, audio-books etc).

O aumento na produção de informação e conhecimento e nossa incapacidade de acompanhá-lo produz o seu oposto: estamos ficando mais "ignorantes". Em particular, com o aumento exponencial da capacidade de processamento e os conceitos envolvidos com o mundo digital, estamos ficando "ignorantes digitais".

Para alguns dos conhecimentos produzidos existe uma sistematização, uma vontade ou uma necessidade maior em sua divulgação e distribuição. Escolas, livros, resenhas, revistas, cursos de especialização etc tentam dar conta deste Tsunami de informação. Infelizmente, a Segurança da Informação não faz parte deste rol.

Some-se a isto tudo o aumento no número de hosts no mundo e, em particular, o aumento do número de usuários de Internet no Brasil para nos dar conta de que o Tsunami não é só de informação mas também de pessoas tendo contato com o ciberespaço.

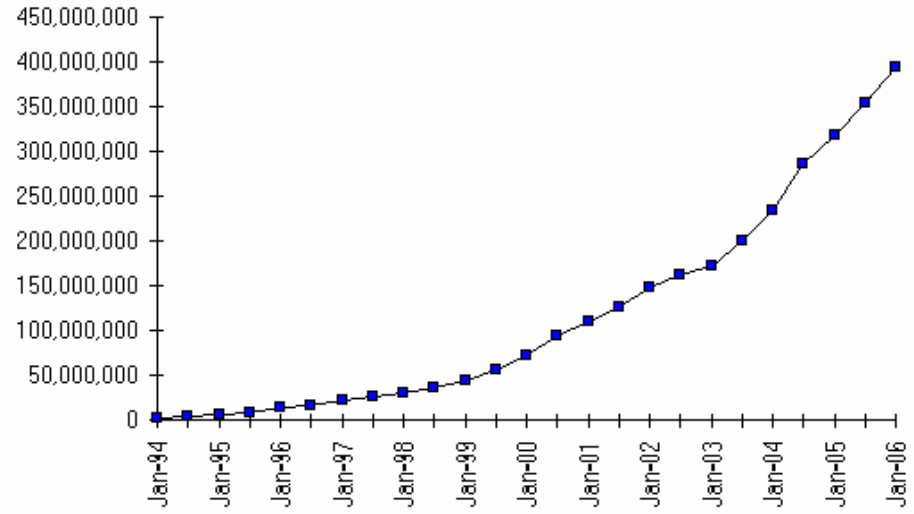

Figura 3 – Evolução no número de Hosts conectados à Internet no mundo
(fonte: Internet Software Consortium, disponível em www.isc.org)

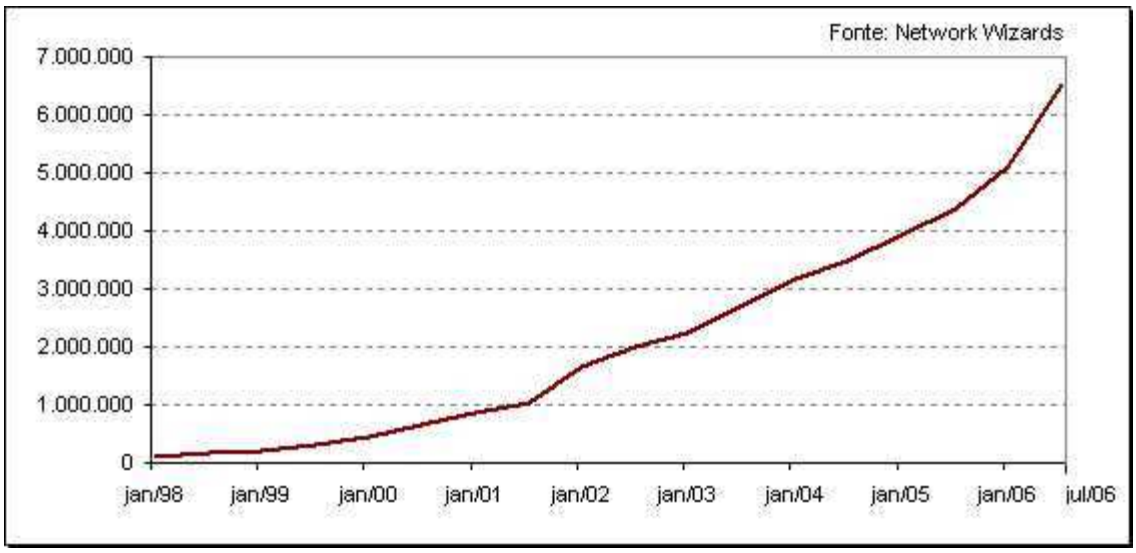

Figura 4 – Evolução do número de hosts no Brasil
(fonte: Network Wizards, disponível em http://www.nic.br/indicadores/hosts/)

QUANTIDADE DE PESSOAS CONECTADAS À WEB NO BRASIL

Série Histórica **1997 -2005**

Data da Pesquisa	População Total	Internautas (milhões)	% da População Brasileira	Crescimento Acumulado (base=jul/97)
2005 /jan	185,6	**25,9**	13,9%	2152%
2004 /jan	178,4	**20,1**	11,5%	1686%
2003 /jan	176,0	**14,3**	8,1%	1143%
2002/ago	175,0	**14,0**	7.9%	1115%
2001/set	172,3	**12,0**	7.0%	947%
2000/nov	169,7	**9,8**	5.8%	756%
1999/dez	166,4	**6,8**	7.1%	490%
1998/dez	163,2	**2,4**	1.4%	104%
1997/dez	160,1	**1,3**	0.8%	13%
1997/jul	160,1	**1,2**	0.7%	-

Tabela 1 – Compilado por www.e-commerce.org.br, (população: variações anuais estimadas)
(fonte: pesquisas diversas, disponível em www.e-commerce.org.br/STATS.htm)

Conjuguemos então todos estes fatores: aumento exponencial da produção de conhecimento, limitações humanas em acompanhar este ritmo, analfabetismo funcional de boa parte da população, inclusão digital realizada sem o devido treinamento/educação, exposição forçada a recursos de computação como ferramentas de trabalho e virtualmente zero de ênfase na Segurança da Informação. O que sai deste caldo de cultura ? Que comportamentos observamos nos usuários destes recursos que mal conhecem o ambiente digital em que trabalham ? Vejamos alguns exemplos:

- Secretária, receosa, ao perceber que seu computador está infectado por um vírus: "Este vírus só pega em computador, né ? Não pega em pessoas não, né ?"
- Técnico (!?) ao comentar que não entendia porque um vírus em seu disquete havia infectado um computador de um cliente: "Mas eu fechei a 'janelinha' do disquete. Ele não tinha como sair (!!!!)".
- Um Professor Doutor reclamando ao helpdesk do mau funcionamento de um computador: "Já liguei e desliguei várias vezes a 'joça' deste computador e a imagem não aparece" (para se descobrir, posteriormente, que o monitor não estava ligado à tomada na parede ou que o controle de brilho do monitor estava no mínimo ...).

Os exemplos acima, ainda que pareçam piadas, são reais e foram presenciados pelo autor. Ainda que não falem exatamente do aspecto de segurança, ilustram o nível dos usuários no início da década de 90. A situação teria melhorado nos últimos anos ?

- Usuário doméstico ao receber a solicitação do atendente do "Auxílio ao Usuário" de que deveria fechar todas as janelas antes de prosseguir: "Já fechei todas as janelas (da casa !!!). E agora ?"
- Um Professor Doutor acerca de firewalls : "Não uso firewall porque meu micro fica muito lento" (mesmo argumento de quem não usa cinto de segurança: "não uso porque é desconfortável").
- Um engenheiro químico sobre antivírus: "Tenho um sim mas está desatualizado" (comparável a quem usa remédio com data de validade vencida)

Os exemplos acima são igualmente reais e presenciados pelo autor. Não, a situação não mudou. E, como mostram os atores das situações acima, a ignorância digital não escolhe camada social nem

formação acadêmica. Falta, é claro, uma educação digital de base e, com ela, uma educação sobre segurança digital (= Segurança da Informação) de base.

Um antigo comercial da década de 80 do microcomputador Hotbit da Sharp mostrava um estudante que, depois de ouvir as maravilhas que o microcomputador poderia fazer por ele, jogava sobre o teclado seu caderno de tarefas dizendo a seguir "Faz aí, faz" ... A noção de que microcomputadores e software existem para "fazer aí", independente do usuário, ainda permanece na cabeça de milhões de pessoas. E mesmo administradores de sistemas continuam achando que máquinas (microcomputadores, redes, firewalls, roteadores) e softwares (antivírus, detetores de intrusão, gerenciadores de controle de acesso) também existem para "fazer aí" a Segurança da Informação de forma independente dos usuários que deles se utilizam.

Voltando a insistir: milhões de usuários têm acesso a recursos de informática sem o mínimo de educação digital necessária, incluindo aí a segurança digital. Eles que têm acesso à Internet via Lan Houses, computadores de correios, microcomputadores promocionais como os do Show do Milhão, ou subsidiados por empresas ou pelo Estado e, futuramente, via laptops de cem dólares que o Governo Federal pretende distribuir entre os estudantes da rede pública. Tudo isso sem um mínimo de treinamento/educação digital. "Clicar e arrastar" é o conhecimento empregado no acesso à Web.

Professores da rede estadual do Estado de São Paulo, por exemplo, foram beneficiados nos últimos anos com um subsídio para compra de computadores pessoais. A iniciativa – louvável – de inclusão digital contemplava ainda a participação em cursos que, anos depois, ainda não foram disponibilizados a vários dos professores que adquiriram e já usam seus computadores.

O investimento, via de regra, é no sentido de se possibilitar o acesso físico aos recursos, sem educar os usuários no bom (e seguro) uso dos mesmos. É o equivalente a garantir o acesso de toda a população a um veículo motorizado sem proporcionar a passagem pelos bancos de uma auto-escola. O desastre é iminente !

Lançadas no ciberespaço sem conhecer seus fundamentos, seus meandros e seus perigos, os usuários acreditam que as máquinas sabem o que estão fazendo e que a segurança é intrínseca ao meio como é intrínseca a qualquer objeto eletrodoméstico. "Se minha TV ou meu microondas são seguros de se usar, a máquina de navegar na Internet também é. Se as máquinas sabem pensar, então eu posso parar de pensar"!

Há um tempo atrás certa mãe preferia desligar o toca-fitas no botão de liga e desliga (em vez da seqüência STOP EJECT ON/OFF) porque não sabia (e não queria) aprender o que eram aqueles

diversos botões PLAY, STOP, Forward, Rewind etc. Hoje, outras mães (e filhos, e pais, e tios, e sobrinhos) preferem apertar YES em toda tela janela que se abre porque não sabem (e não querem) aprender o que está sendo perguntado. “O PC e os programas vão lidar com isto. Se eles pensam, eu posso parar de pensar” !

Quando vemos escolas de ensino infantil, fundamental e médio introduzindo informática em seus currículos parece-nos haver um certa esperança de que tais problemas estejam sendo tratados e de que a educação digital esteja sendo administrada. Muitas destas escolas, porém, se limitam a usar a informática como ferramenta de apoio de algumas matérias de sua grade curricular. Ou apresentam os mesmos cursos “Windows, Word, Excel, Powerpoint e Internet”, sem nenhuma menção aos diversos aspectos de segurança, quais sejam: o sigilo das informações pessoais, o “lado negro” da Internet, as vulnerabilidades dos softwares, os ataques, os crimes informáticos, as ferramentas de proteção como antivírus, firewall, anti-spyware etc. À semelhança do que ocorre com a educação sexual, sem a informação adequada as pessoas tendem a aprender da pior forma possível as conseqüências do uso inadequado dos recursos que lhes são disponibilizados.

Os norte-americanos têm implementado algumas soluções nesta área de educação infantil, como se pode ver em www.safekids.org, www.safeteens.org, www.staysafe.org e outros. Lições a serem aprendidas e seguidas por aqui. Começando pelas crianças e pelos adolescentes, teremos adultos mais conscientes dos riscos de Segurança.

Neste processo de atingir a educação digital há três aspectos que devem ser mencionados:

1. A informática, o ciberespaço e, numa expressão mais ampla, o mundo digital, compõem uma área completamente nova para o indivíduo comum ainda que as pessoas venham tendo contato com ele cada vez mais cedo. Seus mecanismos de funcionamento e seus perigos deveriam ser devidamente apresentados àqueles que com ele têm contato.

2. Algumas vezes nossas noções de segurança no mundo real não são levadas para este mundo digital simplesmente porque sentimos não ser “nossa responsabilidade”. Se um estranho nos perguntar na rua pelos nossos dados pessoais (nome, endereço, telefone, conta bancária, senha do cartão de crédito etc) certamente será dispensado com um “vá passear !”. Se, no entanto, um estranho nos liga no trabalho demonstrando urgência, apresentando-se como um funcionário do helpdesk e solicitando nossa senha para realizar um procedimento qualquer em nosso computador, é bem provável que seja atendido. Afinal, o pior que pode acontecer

é que alguns recursos da empresa serão usados indevidamente ("não é a minha conta bancária em jogo ...").

3. Noutras vezes, é nosso comportamento imprudente do mundo real que é levado para este mundo digital. Da mesma forma que:

   - não usamos cinto de segurança porque incomoda;
   - trazemos o capacete da moto pendurado no braço porque está fazendo muito calor;
   - colocamos a panela com água quente na "boca" mais insegura do fogão porque as demais não aquecem tanto e "pode deixar que eu garanto que a criança por perto não vai se queimar".

   tendemos a:

   - não usar firewalls ou antivírus porque deixam a máquina mais lenta;
   - fornecer senhas pessoais a colegas porque, afinal, "eles têm de trabalhar mesmo que eu não esteja aqui";
   - abrir anexos de e-mails não solicitados mas recebidos de amigos porque "se meu amigo me enviou, então não tem risco, porque ele provavelmente já deve ter aberto também".

Este admirável (e alucinante) mundo novo está em constante atualização. Não conseguimos acompanhá-lo mas somos forçados (e estimulados) a ter contato com ele. Os meios de acesso nos são facilitados mas não o conhecimento para com ele lidar. Não sabemos como ele funciona, nem quais são seus perigos. De forma ingênua achamos que lidar com ele (através das máquinas) é tão seguro quando operar um eletrodoméstico. E que as informações que ele nos provê (e-mails, notícias) são tão confiáveis quando uma carta recebida ou um jornal ou revista publicados. Carregamos em nosso contato com ele os nossos maus hábitos de segurança e poucos ou nenhum de nossos bons hábitos e de nosso bom senso. Paramos de pensar porque achamos que as máquinas já pensam o suficiente.

Agindo assim, o que nos aguarda ?

Perigos e vulnerabilidades: um panorama

Oh, eles têm Internet nos computadores agora.

Homer Simpson, em **Os Simpsons**
(episódio 192, Das Bus), 1998

Quando os microcomputadores faziam jus ao nome de PCs, sendo somente *personal* computers ou computadores *pessoais*, poucos eram os perigos e relativamente pequenos os danos a serem causados. Não conectados, os microcomputadores continham somente informações de seus donos e únicos usuários. Os perigos, quando muito, vinham na forma de disquetes contaminados e, posteriormente, de CDs que junto com jogos carregavam também vírus e cavalos de Tróia.

Nos últimos anos a mudança neste quadro foi radical: conectados, os microcomputadores não só aumentaram a sua capacidade geral de computação como também a capacidade de interação com outras máquinas. Deixaram de ser "personal computers" para ser "cnterprise computers". Empresas começaram a migrar de seus modelos de mainframe/terminais burros para processamento distribuído entre terminais inteligentes. Informação valiosa passou a ser distribuída entre várias máquinas. Conectados, os microcomputadores também viram aumentar exponencialmente os perigos a que estavam sujeitos: a contaminação por disquetes e CDs cedeu lugar à contaminação pela rede. Vírus, cavalos de Tróia, snifers, ataques de negação de serviço, spam, scam, phishing etc passaram a se propagar aproveitando as facilidades, o anonimato e a virtual impunidade permitidos por uma rede mundial de computadores.

Nenhuma máquina está mais a salvo. Excetuando-se o computador da CIA fora da Web em "Missão Impossível" a sala de computadores desconectados da Skynet em "Exterminador do Futuro III" e o computador solitário do abrigo de "Lost", segunda temporada, é difícil encontrar-se um computador que não esteja em rede. E estar em rede é sinônimo de perigo.

Diz-se que um computador seguro é aquele que está desconectado da rede. Nada mais real. A despeito de todas as precauções que possamos tomar, físicas ou de software, jamais poderemos garantir 100% de segurança quando uma máquina estiver conectada numa rede e menos ainda na rede mundial de computadores.

Em setembro de 2006 a BBC News realizou um experimento em que um computador doméstico era deixado conectado à Internet com um ambiente especialmente preparado para registrar todas as

tentativas de ataques a ele. Durante um mês os ataques a ele foram monitorados. Em uma só noite, chegaram a ser registrados 53 ataques. Dentre os ataques, foram registrados :

- tentativas de corromper o servidor Web integrado ao Microsoft Windows
- varreduras de duas portas
- três ataques do worm Slammer
- trinta e seis anúncios falsos ou advertências colocadas por falsos programas de segurança
- pelo menos um ataque por hora tentando se aproveitar de um perigoso erro do Windows
- pelo menos um ataque sério por noite, com tentativas de seqüestrar a máquina e transformá-la em uma máquina zumbi

Segundo o mesmo artigo, a Symantec declarou que 86% de todos os ataques individuais a máquinas são dirigidos contra usuários domésticos[11].

Se nosso foco são as empresas e seus colaboradores, por que nos importar com usuários domésticos ? É que usuários normalmente não têm boas práticas de segurança em casa. E no trabalho eles não se travestem de bons usuários, eles simplesmente repetem comportamentos normais de seu dia-a-dia. Se queremos ter bons usuários (isto é, usuários comprometidos com a segurança) então eles devem ser também bons usuários domésticos, comprometidos igualmente com a segurança de seus computadores e programas em casa.

Ainda assim, com as tecnologias corretas, máquinas corporativas estariam protegidas ? Vejamos:

- Firewalls e roteadores ? Podem estar mal configurados ou com bugs em seu firmware.
- Antivírus, softwares de firewalls ? Podem estar não atualizados ou conterem vulnerabilidades.
- Sistemas operacionais e navegadores abertos ? Foi só uma questão de tempo para que Linux, Konqueror, Opera e Mozilla/Firefox apresentassem suas vulnerabilidades.

[11] " Computadoras hogareñas reciben 50 o más ataques por noche", disponível em http://www.enciclopediavirus.com/noticias/verNoticia.php?id=685

PERIGOS & VULNERABILIDADES

A que perigos estamos expostos no momento em que nos conectamos à uma rede ?

- Vírus: a ameaça mais lembrada em pesquisas com o público em geral.
- Cavalos de Tróia: enquanto os vírus têm uma características destrutiva e, por isto mesmo, facilmente detectável, os cavalos de Tróia trabalham de forma silenciosa roubando informações.
- Spam: de forma irritante, enchem nossa caixa postal com mensagens indesejadas.
- Scam: pegando carona nos spams, têm como objetivo o roubo de informações pessoais que possam se traduzir em vantagem econômica como dados bancários, números de cartão de crédito, senhas, CPF etc.
- Phishing: ainda na carona dos spams, apresentam mensagens aparentemente verdadeiras de empresas idôneas e com as quais o destinatário tenha algum tipo de relacionamento para obter do mesmo informações sensíveis como dados bancários ou números de cartão de crédito.
- Worms: sem necessariamente portar uma carga destrutiva, viajam pela rede consumindo recursos de banda e eventualmente derrubando servidores por ataques de negação de serviço..
- Códigos Active X maliciosos: quando o simples ato de abrir uma página num navegador causa o carregamento de um código destrutivo que pode conter qualquer uma das ameaças acima. O número de ataques de código malicioso, que são utilizados com freqüência para obter dados confidenciais, aumentou quase 50% no último ano[12].
- Spyware/Adware: códigos que rodam na máquina do usuário, sem seu consentimento, coletando informação pessoal do mesmo e enviando tais informações a um computador remoto. De cada 10 computadores, 9 estão infectados com spyware[13].
- Explorações (exploits) de vulnerabilidades conhecidas em softwares comercias

[12] http://www.websense.com/global/pt/ResourceCenter/IndustrySolutions/Technology/
[13] idem. Veja também http://tecnologia.uol.com.br/ultnot/2006/08/28/ult2870u97.jhtm

- Explorações (exploits) de vulnerabilidades conhecidas nas próprias ferramentas de segurança como antivírus e firewalls
- Assinaturas digitais, certificados digitais e arquivos criptografados que podem ser vulneráveis se existir um simples cavalo de Tróia instalado capturando a seqüência de teclas usada para digitar a senha de abertura dos mesmos
- Sistemas de autenticação por senha que se tornam vulneráveis simplesmente porque um usuário não cuidou bem do sigilo de sua senha, escolheu uma fraca ou simplesmente a revelou para outro colega de trabalho só para não ter de voltar à empresa tarde da noite
- Remetentes de e-mails que não são quem dizer ser
- Links em páginas da Internet e em e-mails que não levam para onde se pensa que deveriam levar

Outros perigos nos rodeiam pelo simples fato de termos acesso a informações sensíveis. Mesmo distantes de um microcomputador podemos colocar em risco alguns ativos das empresas para as quais trabalhamos quando:

- Divulgamos informações a pessoas não autorizadas: a engenharia social (a arte de convencer uma pessoa a fornecer uma informação ou realizar alguma ação fazendo-se passar por outra pessoa ou simulando uma situação de urgência) é a primeira colocada no ranking dos ataques a que estamos sujeitos nas palavras do hacker Kevin Mitnick.
- Deixamos de descartar de forma adequada a informação em papel: o que possibilita o uso do dumpster diving, "técnica" (?!) em que o atacante literalmente mergulha no lixo de uma empresa para conseguir informações como senhas, user ids etc. O que ocorreu há alguns anos atrás com criminosos brasileiros que, vasculhando o lixo de um banco, descobriram nomes de correntistas com respectivos números de conta. Tentando algumas senhas fracas (como aquelas que continham partes do nome do correntista, por exemplo, numa senha de 4 caracteres) conseguiram acesso a várias contas corrente.
- Não efetuamos o backup de informações sensíveis presentes somente em nosso computador: quando o processamento era centralizado, era fácil para os responsáveis pelo CPD realizaram de forma rotineira backups diários, semanais ou mensais. Agora com o processamento distribuído, espera-se que os usuários (que jamais tiveram contato com estas boas práticas de mainframe) sejam responsáveis, cada um deles, pelo backup de seus dados

(que, enfatize-se, não são dele mas da empresa para a qual trabalham). Vamos nos demorar um pouco mais neste ponto: num estudo datado de fevereiro de 2006 e encomendado à Harris Interactive pela empresa de segurança de dados Symantec, descobriu-se que quase metade dos usuários de computador não realizam backup de seus dados[14]:

- 57% fazem backup de seus dados
- 51% o fazem de forma regular
- dentre os que não fazem backup, 33% não pensam nisto e 31% sentem que não é importante
- 24% do total perdeu algum tipo de dado nos seis meses anteriores à pesquisa
- razões para perda de dados incluem crash no sistema (11%), apagamento acidental (9%), vírus (9%), falta de organização (3%) e outras (2%).

As ameaças são muitas. E aumentam a cada dia. Não bastam os vírus, spams, scams, phishing, cavalos de Tróia, engenharia social, ausência de backups etc. Outras modalidades aparecem no cenário de forma mais rápida do que podemos entender ou nos precaver. Algumas mais recentes e dignas de nota e que eventualmente prescindem até do uso de um computador:

1. a extorsão digital: a vítima recebe um e-mail dizendo que se determinada quantia não for depositada numa conta terá seu computador inundado com fotos de pedofilia, seguindo-se uma denúncia às autoridades policiais e aos meios de comunicação de massa. Como a quantia solicitada normalmente é pequena, há a tendência de se efetuar o pagamento com receio dos danos irreparáveis à imagem da vítima.
2. o seqüestro de informações: uma empresa sediada em Boston, EUA, no início de 2006, teve um laptop roubado, o qual possuía dados pessoais e financeiros de 196 mil funcionários da HP. No Brasil, outro usuário, após ter seu notebook roubado, recebeu via Orkut um aviso dizendo que o disco rígido havia sido encontrado. Para que o HD fosse devolvido, no entanto, teria de pagar R$ 15 mil. Segundo Marcelo Okano, professor de pós-graduação da FIAP – Faculdade de Informática e Administração Paulista – e especialista em segurança na Web, “uma pessoa mal-intencionada pode roubar ou invadir computadores, capturar

[14] “ Nearly Half of Computer Users Don't Back-Up Data”, disponível em http://www.clickz.com/stats/sectors/software/article.php/3611461

determinados arquivos e depois cobrar para devolvê-los ao dono, ou mesmo utilizá-los para outros fins como a espionagem industrial"[15].

3. o Vishing, variante do phishing, em que o atacante envia um e-mail ou deixa um recado telefônico em uma secretária eletrônica ou caixa postal de voz, orientando a vítima a entrar em contanto telefônico com o seu banco ou administradora de cartões utilizando, no entanto, um número fornecido pelo atacante. Este número telefônico, que se utiliza de um serviço de VoIP (voz sobre IP) contratado com uma dentre várias empresas (como o Skype), pode até estar localizado em outro país. Ao ligar para o número fornecido, a vítima entra em contato com uma central automática que solicita seus dados bancários (ou do cartão de crédito) e os envia posteriormente ao atacante.

   Os usuários estão ficando, pelo excesso de ataques de phishing, inoculados contra clicar em links que vêm em mensagens de e-mail. Esta preocupação, no entanto, não aparece ao se discar para um número fornecido pelo e-mail.

4. o Smishing, variante do phishing e do vishing e que utiliza mensagens SMS enviadas para os aparelhos celulares também solicitando que a vítima entre em contato telefônico com um número fornecido pelo atacante e que se trata, igualmente, de um número VoIP.

Estamos imersos num meio em que cibercriminosos, crackers, engenheiros sociais (estes, no fundo, estelionatários a quem, nas palavras do advogado Renato Opice Blum, impropriamente se concedeu um título de graduação) estão não somente espreitando mas ativamente trabalhando para conseguir acesso a informações valiosas, sejam pessoais sejam empresariais.

Eles exploram falhas em softwares comumente utilizados, enviam e-mails que tentam enganar os mais incautos, ativam worms que atacam sistematicamente sites tornando-os indisponíveis, instalam cavalos de Tróia que capturam os dados digitados em sites de bancos ou de outras instituições financeiras, ou que filmam o movimento do mouse enquanto usam teclados virtuais, e alarmam os mercados enviando e-mails que se parecem ter sido enviados por instituições sérias.

[15] http://www.modulo.com.br/index.jsp?page=3&catid=7&objid=4749&pagecounter=0&idiom=0

PANORAMA (ALGUNS NÚMEROS)

Comecemos com o phishing, aquela ameaça em que um e-mail apresenta um link para uma página falsa de uma instituição real com a finalidade de coletar informações importantes da vítima.

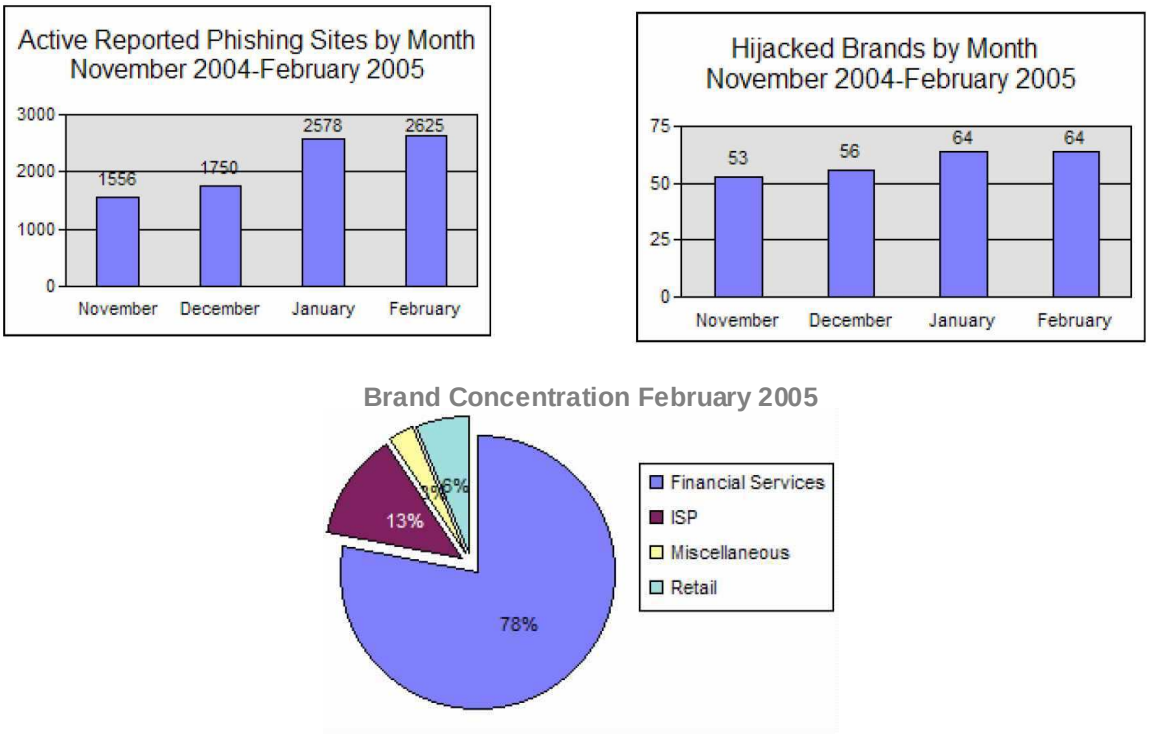

Figura 5 – Panorama dos ataques tipo PHISHING em Fevereiro de 2005
(fonte: Phishing Activity Trends Report, February/2005, disponível em www.antiphishing.org)

Muito significativo é o fato de que três quartos das páginas falsificadas simulavam serviços financeiros (vide gráfico na figura 5).

Como se vê, o malware que tem sido escrito nos últimos anos tem focado diretamente a possibilidade de se conseguir dinheiro de forma rápida. Um acompanhamento feito no primeiro semestre de 2006 pela TruPrevent da Panda Software (Panda Labs) aponta que 94% do malware visava ciberdelitos[16]: cavalos de Tróia (70,7%), bots (17,5%), dialers (4,8%) e spyware/adware (1,5%). Significativo também é que a tendência de se criar worms de ataque massivo tem diminuído: em 2005 foram 40% de worms contra 26% de cavalos de Tróia, enquanto neste primeiro trimestre de 2006 a proporção foi de 4,9% de worms contra 70,7% de cavalos de Tróia. Os ataques têm se dirigido contra objetivos mais concretos e não de forma massiva.

Alguns outros números brasileiros (fonte CGI – Comitê Gestor da Internet no Brasil):

[16] http://www.diarioti.com/gate/n.php?id=12294

- 31% dos usuários de Internet não atualizam seus antivírus.
- Somente 18% dos usuários conseguem enviar um e-mail com um arquivo anexado.
- 56,5% confessam que não têm nenhuma habilidade para uso da Internet ou do computador, enquanto 17% tentam obter estas habilidades por conta própria, prescindindo das demais formais de obtenção de conhecimento (escolas de informática, cursos para adultos, colegas, amigos etc).

Nos capítulos anteriores já falamos do crescimento vertiginoso não só no número de usuários como também no número de hosts na Internet.

O número de máquinas e usuários conectados aumenta exponencialmente a quantidade de ataques que se pode realizar. A propagação é extremamente rápida neste meio, seja por conta da disponibilidade de recursos (vide worm Slammer citado na introdução), seja por conta da falta de informação e educação dos usuários (que sucumbem a ataques de phishing ou outros menos elaborados como os dos cavalos de Tróia, vírus e worms que se propagam com anexos de e-mails com vídeos ou fotos eróticas).

Usuários mal capacitados frente a fontes crescentes e mais direcionadas de perigos e ameaças formam o pano de fundo para o grande problema que é a garantia da Segurança de Informação. Como agir neste cenário ?

Não precisamos de pessoas, resolvemos tudo com tecnologia

Steve Austin, astronauta. Um homem quase morto.
Senhores, nós podemos reconstruí-lo.
Nós temos a tecnologia.
Nós temos a capacidade de construir o primeiro homem biônico do mundo.
Steve Austin será este homem. Melhor do que era antes.
Melhor, mais forte, mais rápido.

Linhas iniciais de **Cyborg, o Homem de Seis Milhões de Dólares**
(The Six Million Dollar Man), 1973

Frente a todos os perigos listados no capítulo anterior, muitos entendem ser razoável não depender do usuário final (ou do fator humano em geral) para garantir a Segurança da Informação.

A tecnologia existente seria suficiente para garantir a segurança: o uso de diferentes redes físicas para acesso à Intranet e à Internet, firewalls, spyware, antivírus, sistemas de detecção de intrusos (os IDS), anti-spam, ausência de CD drivers e floppy disks bem como o bloqueio de pen-drives em todas as máquinas destinadas a usuários, monitoramento de e-mails e do acesso à Internet, sistemas de identificação e autenticação envolvendo senhas fortes, smart cards (ou tokens) e biometria seriam algumas das ferramentas tecnológicas que tornariam possível a segurança 100%.

Dois especialistas em segurança, Marcus Ranum e Bruce Schneier, de forma e com visões diferentes, abordam este assunto em seus escritos.

Marcus Ranum identifica a educação dos usuários como uma das seis idéias mais idiotas na área de segurança de computadores. Na verdade, ele a considera menos que idiota[17]. A citação é longa mas instrutiva acerca de seu pensamento:

"Se fosse para funcionar, já deveria ter funcionado. Têm havido inúmeros estudos interessantes que indicam que uma porcentagem significativa de usuários negociariam suas senhas por um barra de doces[18], e o worm Anna Koumikova nos mostrou que aproximadamente metade da humanidade clicaria em qualquer coisa que alegasse conter cenas de nudez de mulheres semi-famosas. Se 'educar os usuários' é a estratégia

[17] " The Six Dumbest Ideas in Computer Security " , disponível em http://www.ranum.com/security/computer_security/editorials/dumb/

[18] *"Num estudo conduzido pela empresa PentaSafe Security Technologies, dois terços dos trabalhadores entrevistados na estação Vitória em Londres deram ao entrevistador suas senhas quando solicitados. A recompensa ? Uma caneta barata."* (http://news.com.com/2009-1001-916719.html)

na qual você planeja embarcar, você deveria aplicar um 'patch' em seus usuários toda semana. Isto é idiotice.

"A questão real não é perguntar 'nós podemos educar nossos usuários para melhoras nossa segurança ?' e, sim, 'por que afinal nós necessitamos educar nossos usuários?'. Num certo sentido, isto é um caso especial da 'permissão default' - por que os usurários estão recebendo anexos executáveis ? Por que os usuários estão esperando receber e-mails de bancos nos quais eles não têm contas ? A maioria dos problemas que são endereçáveis através da educação dos usuários são auto-corrigíveis ao longo do tempo. Á medida que uma geração mais jovem de trabalhadores entra para o mercado de trabalho, eles já virão 'pré-instalados' com um saudável ceticismo acerca de phishing e engenharia social.

"Lidar com coisas como anexos e phishing é um outro caso de 'permissão default' - nossa idéia idiota favorita. Afinal, se você está deixando todos os seus usuários receberem anexos em seus e-mails você está 'permitindo por default' qualquer coisa que seja enviado para eles. Uma idéia melhor seria simplesmente colocar em quarentena todos os anexos à medida que eles chegam à empresa, apagar de imediato todos os executáveis e armazenar os poucos arquivos que você decidir que sejam aceitáveis num servidor onde os usuários podem se logar com um browser habilitado para conexões SSL para baixá-los (solicitar uma senha para logar vai eliminar vários mecanismos de propagação de worms). Há algumas ferramentas freeware como MIMEDefang que podem facilmente ser utilizadas para remover anexos de e-mails recebidos, armazená-los num diretório individual para cada usuário e substituir o anexo no e-mail por um link para o anexo removido. Por que educar seus usuários para lidar com um problema se você pode simplesmente cravar uma estaca diretamente no coração do problema ?

"Quando eu era CEO de uma pequena empresa de segurança de computadores nós não tínhamos um administrador de sistemas para o Windows. Todos os empregados que queriam trabalhar com o Windows tinham de saber como instalá-lo e como lidar com ele por si mesmos, ou eles não seriam contratados. Minha previsão é de que em dez anos usuários que necessitem educação estarão totalmente fora do mercado de trabalho high-tech, ou estarão obtendo treinamento auto-didático em casa a fim de permanecerem competitivos. Meu palpite é que isto se estenda a saber que não se deve abrir anexos estranhos enviados por desconhecidos."

Em resumo:

1. aplique tecnologia onde você espera por discernimento humano e as coisas irão funcionar; e
2. uma força de trabalho formada por uma geração mais nova já virá vacinada contra a engenharia social.

Bruce Schneier, autor de "Segurança.Com - Segredos e mentiras sobre a proteção na vida digital", também não acredita no fator humano para a segurança de sistemas, computadores e informação. Um dos editoriais que comentam este seu livro o apresenta desta forma:

"Bruce Schneier tem trabalhado com criptografia e segurança eletrônica por anos e chegou à depressiva conclusão de que mesmo o código mais lindo e o hardware mais robusto ainda cederão aos ataques que exploram a fraqueza humana dos usuários".

No livro citado, ele dedica todo um capítulo ao "fator humano"[19]. Sua posição pode ser resumida com algumas citações extraídas daquele capítulo:

"Para este milagroso sistema de computador realizar algo útil, ele terá que interagir com usuários de alguma forma, em algum momento e por algum motivo. E essa interação é o maior risco à segurança de todos eles. As pessoas normalmente representam o elo mais fraco na corrente da segurança, e cronicamente são responsáveis pela falha dos sistemas de segurança.

"As pessoas não entendem computadores. Os computadores são caixas mágicas que fazem coisas. As pessoas acreditam no que os computadores dizem. As pessoas só querem realizar suas tarefas".

Ele enumera seis aspectos do fator humano. Novamente, a longa citação serve para esclarecer seu ponto de vista:

1. Como as pessoas percebem os riscos

   "As pessoas não entendem riscos (...) O problema não é apenas de não ter informações suficientes; as pessoas têm problemas para avaliar riscos mesmo com as informações adequadas."

2. Como as pessoas lidam com coisas que acontecem muito raramente

   "Um perigo dos sistemas computadorizados é que eles cometam erros tão raramente que as pessoas não saibam como lidar com eles (...) 'Eu nunca vi aquela luz vermelha piscando antes, queria saber o que significa...' (...) Infelizmente, se houver muitos alarmes aleatórios, os operadores aprenderão a ignorá-los (...) 'Aquela luz vermelha está sempre piscando e nunca há um problema. Eu simplesmente vou ignorá-lo de novo...'"

3. O problema de usuários confiando em computadores e porque isso pode ser tão perigoso

   "O problema fundamental é que você pode não ter idéia alguma quanto ao que o computador está realmente fazendo quando você lhe diz para fazer algo (...) Se você estiver trabalhando em um computador inseguro – o que acontecerá quase todo o tempo –, não haverá certeza de que aquilo

[19] Segurança.Com - Segredos e mentiras sobre a proteção na vida digital, Editora Campus, 2001, pp. 255 a 268

que você vê é o que você obtém, ou que aquilo que você obtém realmente funciona como você espera."

4. A futilidade de pedir às pessoas para tomar decisões de segurança inteligentes

   "As pessoas querem segurança, mas não querem vê-la funcionando (...) Quando se aproxima um prazo e você precisa terminar o serviço, as pessoas nem pensam duas vezes antes de contornar a segurança. Elas deixarão a porta de incêndio aberta para que alguém possa entrar no prédio com mais facilidade, e passarão a sua senha ou desativarão um firewall porque o trabalho precisa ser feito (...) Não se pode confiar que as pessoas implementarão diretrizes de segurança de computador, trancarão sues carros, não perderão suas carteiras e não contarão a ninguém sobre o nome de solteira de sua mãe."

5. Os perigos dos internos maliciosos

   "A pessoa que escreve um programa de segurança pode colocar uma porta dos fundos nele. A pessoa que instala um firewall pode deixar uma abertura secreta. A pessoa cujo trabalho é realizar a auditoria de um sistema de segurança pode deliberadamente se esquecer de algumas coisas (...) No fim (...) uma organização está à mercê de seu pessoal."

6. Engenharia social e por que é tão fácil para um hacker simplesmente pedir informações secretas

   "A engenharia social (...) é muito eficiente (...) Ela evita a criptografia, segurança de computador, segurança de rede e tudo o mais que for tecnológico. Ela vai diretamente para o elo mais fraco de qualquer sistema de segurança: o pobre ser humano (...) E é por isso que a engenharia social funciona. As pessoas são basicamente prestativas. E elas são facilmente enganadas (...) No fim, engenharia social provavelmente sempre funcionará."

Ambos os especialistas, Marcus Ranum e Bruce Schneier, descrêem do fator humano. Há, porém, uma diferença fundamental entre ambos: Marcus Ranum aposta na tecnologia para compensar a fraqueza do elemento humano na corrente da Segurança da Informação. Já Bruce Schneier descrê, inclusive, da própria tecnologia, como vários dos comentários acima deixam transparecer. Em suma:

- Para Marcus, não adianta investir nas pessoas: pessoas falham, tecnologia não
- Para Bruce, não adianta investir nas pessoas: tecnologias falham, pessoas também

O fator humano realmente não mereceria investimento ? Somente a tecnologia seria suficiente ? Nem a tecnologia seria suficiente ?

Nos capítulos seguintes discutiremos ambos os pontos de vista e ofereceremos uma terceira via.

Tecnologia não é tudo

Entrevistador: HAL, você tem uma enorme responsabilidade nesta missão, em vários sentidos talvez a maior responsabilidade que qualquer outro simples elemento desta missão possa ter. Você é o cérebro, o sistema nervoso central da espaçonave, e suas responsabilidades incluem cuidar dos homens em hibernação. Alguma vez isto te causou alguma falta de confiança ?

HAL 9000: Vamos colocar desta maneira. A série 9000 é o computador mais confiável jamais feito. Nenhum computador 9000 jamais cometeu um erro ou distorceu alguma informação. Nós somos, em todos os sentidos práticos, à prova de e incapazes de erros.

(já no espaço, respondendo sobre uma suposta falha da antena parabólica da espaçonave, a qual o próprio HAL forjou ...)

HAL: Isto só pode ser atribuído a um erro humano.

(... e, logo depois, ao impedir a entrada do astronauta Dave Bowman na espaçonave)

Dave: Do que você está falando, HAL ?
HAL: Esta missão é muito importante para mim para que eu permita que você a coloque em risco.

Diálogos do computador HAL 9000 em **2001: Uma Odisséia no Espaço** (2001: A Space Odyssey), 1968

Em certa medida, confiamos nas máquinas e nos programas que rodam nelas. Digitamos um texto, enviamos um e-mail, calculamos uma planilha ou desenhamos um prédio confiando que o conteúdo do texto não vai ser modificado, que o e-mail vai chegar ao destinatário correto, que os cálculos das planilhas estão corretos e que a estrutura desenhada vai suportar os esforços previstos.

O dia a dia, no entanto, principalmente na área da Segurança da Informação, revela-se um pouco mais confuso. O firewall ou o roteador contém regras que foram fornecidas por um técnico e que podem conter erros. Navegadores de Internet contém bugs e vulnerabilidades que não são corrigidas a tempo com a liberação de patches de segurança por parte dos desenvolvedores. Algumas vezes tais patches não eliminam as vulnerabilidades, ou criam outras, ou fazem reaparecer

vulnerabilidades já corrigidas por um patch anterior. Softwares antivírus e de firewall também carregam bugs e/ou vulnerabilidades.

Voltemos aos navegadores. Freqüentemente se fala que o Firefox/Mozilla é mais seguro que o Internet Explorer/Microsoft. Descansa-se nesta crença para relaxar em outros aspectos da segurança.

Curiosamente, o Laboratório de Pesquisas Navais do Governo dos Estados Unidos, que define a política de segurança dos computadores da Marinha, reprovou o Netscape Navigator no início de 1996 por conta de vários problemas de segurança encontrados naquele produto, adotando em outubro daquele ano o Internet Explorer da Microsoft como seu navegador oficial[20].

A questão não é saber se o navegador (ou um software em geral) é seguro ou não, e sim quando suas vulnerabilidades começarão a ser exploradas. Aconteceu com o Internet Explorer, está acontecendo com o Firefox[21]. Citando novamente Bruce Schneier, *"é inconcebível que uma grande aplicação na Internet seja livre de bugs"*[22].

Os mesmos comentários se aplicam a outros sistemas operacionais, como o Unix ou Linux, e sistemas operacionais que rodam sobre outras plataformas[23].

Voltemos a um dos argumentos de Marcus Ranum citados no capítulo anterior: remover anexos de e-mails indesejáveis antes de eles chegarem aos destinatários finais. Digamos que a política da empresa não permita arquivos executáveis, compactados, batches, documentos com macros, htmls etc. Se o destinatário, no entanto, solicitar ao remetente que renomeie o anexo para que contenha uma extensão inocente, como .txt ou .jpg, de nada adiantou a tecnologia do filtro.

Acerca de outro comentário de Marcus Ranum, de que seria idiotice reforçar a segurança de informação através da educação de usuários, lembramos que os administradores de sistemas, que em última análise implementam as políticas de segurança, eles mesmos também são usuários: usuários de sistemas operacionais, de programas de segurança e da infra-estrutura da rede. A parametrização dos diversos programas, o estabelecimento de regras de filtragem, a atualização dos

[20] Comércio & Segurança na Web, Editora Market Books Brasil, 1999, pp. 37 e 38
[21] vide, por ex., http://www.idgnow.com.br/seguranca/2004/12/09/idgnoticia.2006-05-07.6481023573, http://www.idgnow.com.br/seguranca/2005/06/07/idgnoticia.2006-03-12.1432284974, http://www.idgnow.com.br/seguranca/2005/12/13/idgnoticia.2006-03-12.1141923058 e http://www.idgnow.com.br/seguranca/2006/06/29/idgnoticia.2006-06-29.5013809678
[22] Segurança.Com - Segredos e mentiras sobre a proteção na vida digital, Editora Campus, 2001, p. 208
[23] http://idgnow.uol.com.br/seguranca/2006/04/19/idgnoticia.2006-04-19.8261984789/IDGNoticia_view e http://idgnow.uol.com.br/seguranca/2006/05/15/idgnoticia.2006-05-15.0362530644/IDGNoticia_view

diferente softwares, tudo passa por pessoas. Este autor teve a experiência de alertar um administrador de sistemas de uma conhecida livraria online a respeito de um certificado de segurança com prazo de validade vencido e de ver que, dias após, as páginas ainda estavam no ar com o mesmo certificado vencido.

No já referido exemplo do worm Slammer, sua propagação só ocorreu porque haviam produtos com uma falha de segurança conhecida e um patch liberado para corrigi-las que não fora instalado. Vemos aqui, em primeiro lugar, uma falha dos administradores de sistemas, que ignoraram a necessidade de se proceder a uma atualização dos softwares envolvidos. Por outro lado, cabe perguntar o porquê desta aparente negligência.

Muitos administradores são reticentes em aplicar de imediato patches de segurança recém-liberados porque muitas vezes tais patches:

1. simplesmente não funcionam[24];
2. carregam consigo outros problemas que tornam sistemas anteriormente estáveis em instáveis[25];
3. introduzem uma vulnerabilidade nova no software atualizado[26]; e
4. fazem reaparecer vulnerabilidades antigas[27].

Pedro Antonio Dourado de Rezende, Professor do Departamento de Ciência da Computação da Universidade de Brasília, em excelente artigo no "Observatório da Imprensa" comentando o caso do worm Slammer cita, dentre diversos aspectos:

1. que o patch da Microsoft não resolveria 100% do problema;
2. que atualizações de 100% dos produtos afetados seria custosa demais ferindo prioridades;
3. que atualizações 100% carregam riscos como os enumerados mais acima;

[24] http://www.enciclopediavirus.com/noticias/verNoticia.php?id=280
[25] http://news.zdnet.com/2100-1009_22-5648595.html, http://www1.folha.uol.com.br/folha/informatica/ult124u12520.shtml e http://idgnow.uol.com.br/seguranca/2006/08/21/idgnoticia.2006-08-21.3759090119/IDGNoticia_view
[26] http://idgnow.uol.com.br/seguranca/2006/08/22/idgnoticia.2006-08-22.8489954397/IDGNoticia_view
[27] *"Também é mais que habitual (em mais ocasiões do que pensamos e 'nas melhores famílias') introduzir 'erros de regressão' nas soluções. Isto se produz quando um patch soluciona algum problema de segurança mas também, como efeito colateral, abre alguma antiga vulnerabilidade fechada em qualquer outro momento por outro patch"*, disponível em http://www.hispasec.com/unaaldia/2860

afirmando, por fim, que *"pode-se condenar a hipocrisia dos que persistem em julgamentos simplistas sobre as responsabilidades"*. Em outras palavras, os problemas vão além da tecnologia e da responsabilização pura e simples de usuários e administradores.

Ainda que as empresas adotem boas práticas de segurança baseadas em tecnologia (pensando, assim, cobrir a insegurança inerente aos usuários) um amplo espectro de perigos e vulnerabilidades não é totalmente coberto (ou resolvido):

- engenharia social ataca os usuários, não a tecnologia (para Simson Garfinkel e Gene Spafford, *"não existe uma solução ideal para ataques de engenharia social que não seja a educação"*[28])
- os usuários, quando precisam e querem, burlam os controles de segurança
- sistemas de autenticação requerem senha, mas se estas forem fracas, podem ser facilmente identificadas e utilizadas
- senhas fortes podem ser impostas mas elas são difíceis de se guardar na memória
- facilidade de uso para os usuários e segurança são objetivos que muitas vezes se contrapõem
- usuários com acesso remoto podem ter suas máquinas não corretamente configuradas ou atualizadas
- quando necessário, os usuários divulgam suas senhas a colegas para facilitar o trabalho de ambos[29]
- vulnerabilidades aparecendo de forma contínua vão tornando obsoletos alguns dos controles tecnológicos
- ausência de políticas de backup
- funcionários negligentes que se afastam de seus computadores sem bloquear o acesso à tela ou ao teclado
- uso de sistemas operacionais que permitem acesso sem o necessário login

[28] Comércio & Segurança na Web, Editora Market Books Brasil, 1999, p. 35
[29] *"num estudo conduzido pela empresa PentaSafe Security Technologies, 4 de cada 5 trabalhadores revelariam suas senhas para outra pessoa em sua companhia se fossem solicitados a fazê-lo"* (http://news.com.com/2009-1001-916719.html)

- sistemas operacionais que, ainda que solicitem login, contém bugs eliminam a necessidade deste login[30]
- filtros ineficazes de e-mails
- vazamento de informações como aquele supostamente ocorrido com dados da declaração de renda de 2004 no Brasil[31]

Vamos analisar dentre as vulnerabilidades tecnológicas acima a questão das senhas. Senhas são o ponto mais fraco do elo mais fraco (o fator humano) da corrente da Segurança da Informação.

[30] http://www.vsantivirus.com/vul-xp-cd.htm
[31] Jornal Nacional, Rede Globo de Televisão, edição de 22/03/2006 (http://jornalnacional.globo.com/Jornalismo/JN/0,,AA1162628-3586,00.html)

O problema das senhas fracas é tão conhecido que Hollywood por vezes brincou com este assunto em suas produções. Vejamos alguns exemplos:

(Jack Ryan da CIA e Dan Murray do FBI conversam com Petey, um especialista em computação da CIA que está ao computador tentando quebrar a senha de um disquete apreendido de uma vítima)

PETEY: Vamos começar com aniversários. *(... e dirigindo-se a Jack)* Aposto que a senha para a conta de seu banco é a data de seu aniversário.
JACK: Quase *(dando as costas e afastando-se junto com Dan).*
PETEY: De trás para frente ?
(Jack pára e volta-se lentamente. Petey ri)
PETEY: OK, o aniversário dele é ... *(e digita alguns números. Percebendo que não deu certo ...)* Isso seria muito fácil, não ? Vamos tentar de trás para frente.
PETEY: Não. O aniversário da mulher dele ? *(digita outros números)*
PETEY: Não. O aniversário do filho dele ? *(continua digitando)*
JACK: Isto pode levar ...
DAN: ... meses.
(Jack e Dan dão as costas e se afastam de Petey)
PETEY: O aniversário do filho dele de trás para frente. *(continua digitando)*
PETEY: Não. O da mulher de trás para frente. *(e, dirigindo-se a Jack ...)* Esta é por você.
PETEY: Não. O da filha de trás para frente.
DAN: *(dirigindo-se a Jack, ambos distantes de Petey)* Você vai ter de mudar a senha no seu banco.
PETEY: Consegui ! *(Jack e Dan param e se voltam para Petey)* Dia do nascimento da filha, mês de nascimento da esposa, ano de nascimento do filho. *(e, dirigindo-se a Jack ...)* Mas não foi de trás para frente. Sinto muito.

Perigo Real e Imediato
(Clear and Present Danger), 1994

(O Rei Roland cede às ameaças de Dark Helmet e começa a dizer a ele a senha do "escudo de ar")

ROLAND: Um.
DARK HELMET (repetindo): Um.
CORONEL SANDURZ (anotando): Um.
ROLAND: Dois.
DARK HELMET: Dois.
CORONEL SANDURZ: Dois.
ROLAND: Três.
DARK HELMET: Três.
CORONEL SANDURZ: Três.
ROLAND: Quatro.
DARK HELMET: Quatro.
CORONEL SANDURZ: Quatro.
ROLAND: Cinco.
DARK HELMET: Cinco.
CORONEL SANDURZ: Cinco.
DARK HELMET: Então a senha é um, dois, três, quatro, cinco ? É a senha mais estúpida que eu jamais ouvi em minha vida. É o tipo de senha que um idiota teria em sua valise de mão.

(Skroob entra no recinto)
SKROOB: Bem, funcionou ? Onde está o rei ?
DARK HELMET: Funcionou, senhor. Nós temos a senha.
SKROOB: Ótimo. Agora nós podemos tomar cada sopro de ar fresco do planeta Druidia. Qual é a senha ?
CORONEL SANDURZ: Um, dois, três, quatro, cinco.
SKROOB: Um, dois, três, quatro, cinco ? Isto é espantoso. Eu tenho a mesma senha na minha valise de mão.

S.O.S Tem Um Louco Solto No Espaço
(Spaceballs), 1987

(Depois de aprender com alguns amigos que sistemas são freqüentemente desenhados com uma "porta dos fundos", de forma que o programador possa penetrar neles com uma senha própria, David investiga a vida do projetista daquele sistema, Professor Falken, e descobre que ele perdeu seu filho Joshua ainda quando criança)

David tenta se logar no sistema novamente, na presença de Jennifer, e desta vez a senha "Joshua" dá a ele acesso ao computador. Ele é então recepcionado com o prompt "Saudações, Professor Falken".

Jogos de Guerra
(War Games), 1983

(alguns hackers conversam num bar com um principiante, Joey)

JOEY: Vocês sempre acham que eu deveria saber tudo e vocês nunca me contam nada. Tô certo ?
PHREAK: Tudo bem. Quais são as três senhas mais comumente usadas ?
JOEY: AMOR, SEGREDO e, uh, SEXO. Mas não necessariamente nesta ordem, certo ?
CEREAL KILLER: É, mas não se esqueça de DEUS. Operadores de sistemas adoram usar DEUS. É aquela coisa de ego do homem.

Hackers – Piratas de Computador
(Hackers), 1995

Senhas fracas fazem parte da natureza humana porque são fáceis de se guardar. Se são fáceis de guardar, também são fáceis de serem adivinhadas, ou deduzidas, ou mesmo tentadas várias vezes em ataques de força bruta utilizando computadores e dicionários de palavras comumente usadas. Usando um conhecido programa chamado "Jack, o estripador" a empresa de proteção de redes Neohapsis levou apenas uma hora para decifrar 30% das senhas de um total de 10.000 contas contidas no arquivo de senhas de uma companhia de serviços médicos[32].

Para contornar este problema, os administradores poderiam utilizar sistemas que forçassem os usuários a:

- utilizar senhas fortes, estabelecendo por exemplo um número mínimo de 8 caracteres e a obrigatoriedade de misturar letras maiúsculas e minúsculas além de números e caracteres especiais (como , . / ? ; @ # $ % ¨& * [ ] etc).
- mudar a sua senha com freqüência (digamos, semanalmente)

Assim, a cada semana o acesso a todos os sistemas seriam bloqueados até que o usuário entrasse com uma nova senha forte que atendesse os requisitos acima.

Ocorre que senhas fortes são difíceis de se lembrar. Poderiam ocorrer alguns problemas aqui:

- o usuário poderia gerar uma senha tão difícil que se esqueceria facilmente dela, o que criaria um grande número de solicitações para a área de TI zerar a senha de usuários
- o usuário passaria a anotar a senha, em vez de memorizá-la, o que comprometeria o seu segredo
- o usuário geraria uma senha fraca disfarçada de senha forte, como o seu próprio nome com letras alternadas maiúsculas e minúsculas, seguido de sua data de nascimento.

O que se quer demonstrar aqui é a ineficácia do uso de tecnologias e do estabelecimento de políticas de segurança que não levam em conta o fator humano. Mais lógico aqui seria aumentar a segurança usando um segundo meio de identificação (a autenticação de fator 2) como os tokens, smart cards, biometria etc. Soma-se algo que a pessoa sabe (senha) com algo que ela tem (cartão) e/ou algo que ela é (biometria). Sistemas vulneráveis usam apenas um tipo de autenticação (algo que se sabe ou algo que se tem ou algo que se é). No dizer do especialista brasileiro Marcos Sêmola, sistemas seguros utilizam dois fatores. E sistemas paranóicos usam três ...

[32] http://news.com.com/2009-1001-916719.html

Existem outros sistemas de autenticação como aqueles em que o usuário escolhe um conjunto de imagens gráficas, dentre um conjunto maior a ele apresentado, como sua senha[33].

É tecnologia mais fator humano, e não somente tecnologia. A gerência e a alta gerência devem ajudar entendendo que não é só culpar o fator humano mas entendê-lo e agir de acordo com este conhecimento.

Além dos exemplos citados envolvendo tecnologia, há um sem número de situações que envolvem Segurança de Informação e que não guardam relação alguma com a tecnologia, dependendo tão somente de um mau comportamento do usuário para trazer prejuízos.

Vejamos a figura abaixo que compõe um Jogo da Segurança (ou jogo dos erros com 24 ameaças e vulnerabilidades) formulado pela Módulo Consultoria[34]:

Figura 6 – Jogo da Segurança
(Modulo © Copyright 2004)

[33] Rachna Dhamija e Adrian Perrig, estudantes na Universidade da Califórnia em Berkeley discutem num recente paper a possibilidade de um sistema gráfico de senhas chamado Deja Vu. (citado em http://news.com.com/2009-1001-916719.html e encontrado em http://www.deas.harvard.edu/~rachna/papers/usenix.pdf)

[34] http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=3008&pagecounter=0&idiom=0

Vamos levantar algumas das ameaças e vulnerabilidades deste ambiente que, repita-se, nada tem a ver com tecnologia[35]:

1. visitas tendo acesso à área de trabalho onde funcionários lidam com informações sigilosas
2. acesso indevido a sites de entretenimento
3. uso de jogos
4. uso de post-its com senha e nome de usuário anotados e visíveis
5. documentos em papel de caráter oficial jogados no lixo sem o devido descarte ou destruição
6. funcionário revelando sua senha ao telefone
7. xícara de café sobre arquivos de backups
8. equipamento de alarme desligado
9. fornecimento de arquivos a pessoa não devidamente identificada cujo crachá está oculto
10. informações de acesso como nome e senha de usuário visíveis na tela de um computadores

Como se vê, em todas as situações acima o fator humano teve uma participação fundamental. Não há o que se possa fazer nestes casos para aumentar a segurança deste ambiente corporativo que não seja a educação e o treinamento de seus funcionários.

Voltando aos comentários de Marcus Ranum citados no capítulo anterior de que seria idiotice educar usuários porque a tecnologia resolveria tudo, a conclusão é de que não somente a tecnologia também falha mas também o usuário pode colaborar para sua falha. Com relação às outras observações suas:

- *"se [educar usuários] fosse para funcionar, já deveria ter funcionado"*: errado, porque os usuários não foram educados (vide Introdução) e os novos usuários não estão recebendo esta educação.
- *"Á medida que uma geração mais jovem de trabalhadores entra para o mercado de trabalho, eles já virão "pré-instalados" com um saudável ceticismo acerca de phishing e engenharia social"*: errado, porque se a geração mais nova carrega consigo um ceticismo maior com relação a certas práticas também carrega outros comportamentos que, se não (re-) educados, farão

[35] para uma relação completa das ameaças e vulnerabilidades deste ambiente, veja http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=3027&pagecounter=0&idiom=0

com que venham a cair em novas técnicas de engenharia social. Afinal, são seres humanos que gostam de ser prestativos. Ao entrarem em contato com o phishing, não necessariamente aprenderam a se precaver contra o vishing ou contra o smishing. A educação de base, de como funciona a engenharia social, é que mudaria este comportamento ingênuo.

- *"Meu palpite é que isto se estenda a saber que não se deve abrir anexos estranhos enviados por desconhecidos"*: em dez anos, as técnicas dos chamados engenheiros sociais já terão se desenvolvido para se adequar a esta nova geração. Sem educação apropriada, esta geração não estará preparada para tais desafios. Além disto, temos de conviver com *esta* geração até que a outra entre no mercado de trabalho. E o que fazer enquanto isto ?

Por várias das razões enumeradas neste capítulo é que Bruce Schneier não só desacredita das pessoas mas também da capacidade da tecnologia oferecer segurança 100%. E isto por dois motivos:

- a segurança depende da tecnologia, e esta falha.
- mesmo que a tecnologia não falhasse, a segurança depende em última análise das pessoas, e estas não são absolutamente confiáveis.

Vejamos outras de suas opiniões:

"A criptografia é um punhado de matemática. E, como toda a matemática, ela envolve números, equações e lógica. Segurança (...) envolve pessoas: coisas que as pessoas conhecem, relacionamentos entre pessoas e como elas se relacionam com as máquinas. A segurança digital envolve computadores: computadores complexos, instáveis e com bugs.

"A matemática é perfeita; a realidade é subjetiva. A matemática é definida; os computadores são teimosos. A matemática é lógica; as pessoas são irregulares, caprichosas e pouco compreensíveis.

"Para a minha surpresa inicial, descobri que os pontos fracos não tinham nada a ver com a matemática. Eles estavam no hardware, no software, nas redes e nas pessoas."

Para ele, à primeira vista os elos são fracos demais. A solução residiria então em aumentar o perímetro de segurança tendo segurança em profundidade: se uma barreira falhasse, outra em seguida conteria aquela falha de segurança.

Segurança em profundidade é um dos conceitos que Bruce Schneier advoga, já que para ele qualquer mecanismo de segurança pode falhar individualmente. Seu estudo destas falhas, exaustiva e didaticamente apresentado em "Segurança.Com - Segredos e mentiras sobre a proteção na vida digital" comprova que não existe um só mecanismo de segurança que possa se mostrar 100% seguro.

Expandindo este conceito, ele discute que mesmo segurança em profundidade não consegue tornar um sistema 100% seguro, motivo pelo qual ele advoga o uso de contramedidas tanto para recuperar eventuais prejuízos como para dissuadir eventuais e futuros atacantes.

Não por acaso depois de trabalhar por anos na área de segurança e criptografia ele veio a fundar a empresa Counterpane Internet Security, Inc, atuando justamente na área de contramedidas (monitoração de segurança gerenciada).

Contramedidas são eficazes judicialmente e como elemento dissuasor para ataques externos (e internos) mas não os impedem e talvez nem sejam capazes de repor os eventuais prejuízos.

Por outro lado, não existem contramedidas dissuasoras para a falta de educação ou de conhecimento. Voltando ao exemplo de Chernobil citado na introdução: o desligamento de controles automáticos (ou a limitação do que eles poderiam fazer), o desligamento dos alarmes, o desprezo às indicações de falha provenientes da falta de conhecimento do correto funcionamento não podem ser endereçadas somente com contramedidas. Contramedidas também podem ser desligadas.

Se nada é 100% seguro, haveria então algum motivo para se investir nas pessoas ? E o que dizer daqueles seis aspectos do fator humano levantados por Bruce Schneier e citados no capítulo anterior ?

1. Como as pessoas percebem os riscos
2. Como as pessoas lidam com coisas que acontecem muito raramente
3. O problema de usuários confiando em computadores e porque isso pode ser tão perigoso
4. A futilidade de pedir às pessoas para tomar decisões de segurança inteligentes
5. Os perigos dos internos maliciosos
6. Engenharia social e por que é tão fácil para um hacker simplesmente pedir informações secretas

O fator humano apresenta realmente todos os aspectos por ele citados. A solução, no entanto, não é prescindir totalmente das pessoas e adotar somente tecnologia ou contramedidas em seu lugar. Todos os elos desta corrente têm suas falhas. Um misto de educação continuada e de recursos tecnológicos é que deve ser implementado. No final, novamente, nem só tecnologia sem só fator humano, mas ambos para fortalecer a corrente da segurança. E, entre os dois, se o fator humano é que é o mais fraco, nele deveriam ser colocados grandes (ou, eventualmente, os maiores) esforços.

Simson Garfinkel e Gene Spafford comentam que *"a segurança na Web não é uma questão de 'tudo ou nada' – a segurança é uma questão de nível. Quanto mais medidas de segurança você emprega, a menos riscos estará sujeito. Seu objetivo deve ser reduzir o risco tanto quanto seja prático (e possível), e depois tomar medidas adicionais para que se algum incidente de segurança ocorrer, você possa restabelecer-se rapidamente"*[36].

Entendo que o fator humano é a primeira barreira ou a primeira linha de defesa a ser vencida (e que pode ser a única ou última dependendo do tipo de ataque). Investimentos pesados em tecnologia, infra-estrutura, equipamento, criptografia etc caem por terra quando o funcionário abre em sua máquina um vírus, quando um administrador de sistemas deixa de instalar um patch de segurança para uma vulnerabilidade conhecida e que é explorada por um hacker mal-intencionado ou mesmo quando uma senha 1-2-3-4-5 é escolhida para acessar um sistema.

[36] Comércio & Segurança na Web, Editora Market Books Brasil, 1999, p. 24

Reforçando a defesa

Quanto mais educação, melhor. É o que eu sempre digo.

Professor Mark Thackeray, em **Ao Mestre Com Carinho**
(To Sir, With Love), 1967

Para introduzir este capítulo, vamos resumir o que já foi dito nos precedentes citando três artigos que trazem, todos eles, o sugestivo título de "O elo mais fraco":

1. *"'A causa primária de quebras na segurança – o fator humano – não está sendo adequadamente endereçada' segundo Brian McCarthy, Chied Operating Officer da ComPTIA (Computing Technology Industry Association). 'A pessoa na frente do PC continua sendo a área primária onde as fraquezas são expostas'"*[37].

2. *"Sistemas de segurança feitos para proteger computadores e redes de investidas criminosas são desenhados por PhDs, codificados por especialistas de segurança com grau de mestrado e integrados nos ambientes corporativos de computação por técnicos habilitados treinados especificamente para aquele propósito. Neste especializado processo de segurança os usuários são freqüentemente esquecidos no fim. O fato simples e triste é que a probabilidade de se quebrar um código feito por um professor de matemática é muito mais baixa do que a probabilidade de se conseguir a senha da secretária de um chefe numa conversa. Se você fosse um atacante, onde você colocaria sua energia ?*

   "Como seria de se esperar, os bandidos colocam sua energia em atacar pessoas. Atacar tecnologicamente um computador ou uma rede requer habilidades especiais, conhecimento, cérebro, tempo e perseverança. Atacar os mesmos objetos de forma psicológica requer somente um gastar de sola dos sapatos. Todos nós temos instalado antivírus, firewalls e outros softwares de segurança destinados a nos proteger contra ataques tecnológicos. Nenhum firewall disponível, de fato nenhum software disponível pode proteger contra um ataque a pessoas. Não há uma bala mágica. Ao invés, treinamento e conscientização são os únicos meios reais de fortalecer o elo mais fraco.

   "Amadores atacam sistemas, profissionais atacam pessoas (...) Em realidade, ninguém pode depender da tecnologia para se fechar a porta aos ataques. Nenhuma solução de software pode resolver todos os problemas de segurança de computador que nos assombram, não importa o que o vendedor de software diga. Nós podemos depender somente de nós mesmos. No fim do dia, um

[37] " The weakest link in the security chain? You" em http://www.silicon.com/research/specialreports/ecrime/0,3800011283,39158023,00.htm

computador é tão seguro quanto a pessoa que o utiliza esteja consciente e pronta para enfrentar os perigos que ela terá de encarar"[38].

3. *"'Pessoas são o elo mais fraco', disse Chirs Pick, vice presidente de estratégia de mercado da empresa de gerencia de sistemas e segurança NetIQ e co-fundador da Human Firewaal, um Web site educacional e informativo agora operado pela ISSA (Information Systems Security Association). Para ele, 'educação é a primeira linha de defesa'.*

   "As empresas estão se tornando cada dia mais conscientes dos problemas que as quebras na segurança e os vírus podem trazer, mas poucas estão investindo dólares em educar a força de trabalho – os últimos guardiões"[39].

Os "últimos guardiões", "a primeira linha de defesa", "a pessoa na frente do PC": treinar, educar ou conscientizar ?

Em interessante trabalho apresentado num Workshop da IEEE em Garantia e Segurança da Informação[40], W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale e Don Welch apresentam o processo de aprendizagem como um *continuum* que se inicia com a conscientização, passando pela "alfabetização" (aquisição de conhecimentos básicos), treinamento e terminando com a educação.

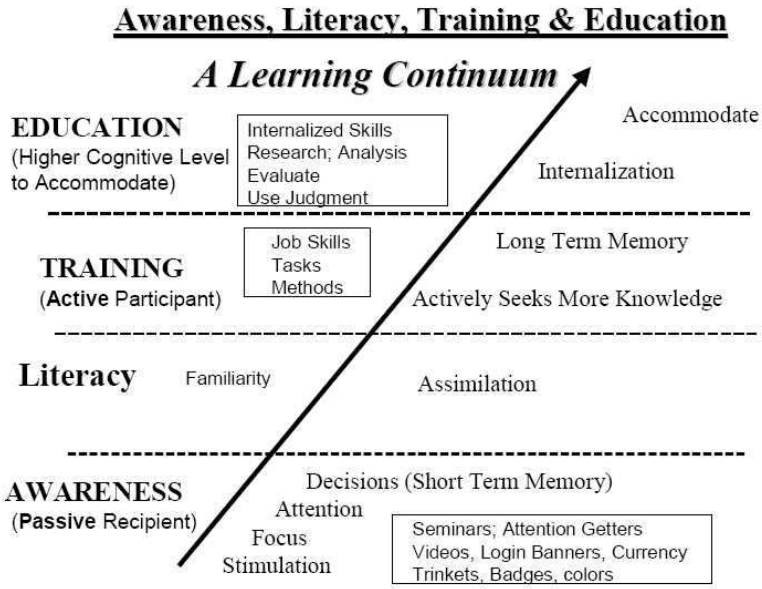

Figura 7 – Processo de aprendizagem

Vamos discutir cada um destes patamares do processo de aprendizagem.

[38] " The Weakest Link" em http://prescientconsulting.com/content/view/43/30/
[39] " The weakest security link? It's you" em http://news.com.com/2100-7355_3-5278576.html

CONSCIENTIZAÇÃO

O primeiro passo em direção a se obter ambientes mais seguros é conscientizar ou sensibilizar os funcionários acerca deste problema. "O problema existe, logo ou sou parte dele ou parte da sua solução" deveria ser o resultado obtido ao fim deste processo.

Outra alvo a ser alcançado diz respeito a como o usuário enxerga o seu comportamento com relação à Segurança da Informação da empresa em que ele trabalha. Se o usuário é cuidadoso com as suas próprias informações e ativos pessoais deveria sê-lo também com as informações e ativos da empresa para a qual trabalha. Ele, por exemplo, não entrega a chave de seu carro a nenhum desconhecido nem tampouco revela a senha de seu banco à pessoa que está na fila do caixa automático. Da mesma forma, não deveria deixar documentos de caráter sigiloso à vista nem tampouco dizer a senha de seu computador a um estranho que, pelo telefone, se diz funcionário do Help Desk.

Ao se falar em processos de melhoria costuma-se dizer que o que não pode ser medido não pode ser melhorado, o que equivale a dizer que só se deve investir naquilo que se pode medir. Neste sentido, a conscientização geralmente é deixada de lado visto que não haveria como se medir o quanto aumentou a "consciência" dos funcionários.

Deve-se dizer, no entanto, que dificilmente se consegue o comprometimento de alguém que não sabe ou não entende o que se requer dele num ambiente corporativo, e quais são os perigos e ameaças a que ele está sujeito. Todo processo "mensurável" de aprendizado deveria necessariamente começar com a conscientização[41].

Interessante notar que a Norma Internacional de Segurança ISO/EIC-17799, que no Brasil se tornou a NBR ISO/EIC-17799, evoluiu na sua compreensão do aspecto humano ao renomear sua

[40] " A Model for Information Assurance: An Integrated Approach", publicado em "Proceedings of the 2001 IEEE Workshop on Information Assurance and Security" e disponível em http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2C3(55).pdf

[41] Os dados são da pesquisa Phishing Trends de 2005*: "58% dos tomadores de decisão em TI entrevistados possuem um programa de conscientização ou um programa de treinamento sobre segurança na Internet, ou ambos. As empresas maiores tendem a fazer mais em termos de segurança da Internet - entre os entrevistados, metade (50%) daqueles que trabalham em empresas de médio porte (definidas como empresas com 100 a 500 funcionários) disse que não possui nenhum tipo de programa de treinamento ou de conscientização, versus 36% dos que trabalham em grandes empresas (501 a 1.000 funcionários) e 29% dos que trabalham para empresas muito grandes (1.001 funcionários ou mais)"*. Os números no Brasil são um pouco piores, segundo a "Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil 2005" do CGI Brasil, disponível em http://www.nic.br/indicadores/indicadores.pdf: *"dentre as empresas consultadas, 19,69% possuem um programa de treinamento em segurança da informação, sendo que este número é superior a 40% nas empresas com mais de 500 funcionários"*

seção "Educação e treinamento em segurança da informação" para "Conscientização, educação e treinamento em segurança da informação"[42].

Para o Auditor de Sistemas Fernando Nicolau Freitas Ferreira (CISM - Certified Information Security Manager pelo ISACA e BS 7799 Lead Auditor pela BSI) "*a garantia de que uma organização possuirá um grau de segurança razoável está diretamente ligado ao nível de conscientização de seus colaboradores, ou seja, a segurança somente será eficaz se todos tiverem pleno conhecimento do que lhes é esperado e de suas responsabilidades*". Para ele, o treinamento e a conscientização em segurança são considerados tanto controles preventivos (já que todos tomam ciência de suas responsabilidades em preservar a segurança física e lógica da organização) como controles detectivos (uma vez que, encorajam os colaboradores a identificar e reportar as possíveis violações de segurança)[43].

Álvaro Teófilo, gerente-geral de Segurança da Informação do banco Santander Banespa, também defende que o passo mais importante no processo de assegurar o macro controle de Segurança em Recursos Humanos é obter a conscientização dos colaboradores. Ele aconselha *"que a maioria das empresas faça iniciativas de segurança com foco nas pessoas"*. Durante o processo de implantação da NBR ISO/EIC-17799 na Caixa Seguros, onde Álvaro trabalhou como Gerente Executivo de Segurança da Informação, havia toda semana uma palestra para os colaboradores sobre um tema de segurança[44].

Este processo de conscientização deve começar já com a orientação dos novos colaboradores. A conscientização não só dele mas dos demais colaboradores pode ser alcançada com o uso de vários recursos, dentre eles os boletins informativos, campanhas, provas periódicas ou entrevistas para avaliar o conhecimento obtido etc.

---

[42] NBR ISO/EIC 17799:2001, Seção 6.2.1 comparada com a NBR ISO/EIC 17799:2005, Seção 8.2.2.
A versão final da NBR ISO/IEC 17799 é uma "tradução literal" da norma Internacional de Segurança da Informação - ISO/IEC-17799, tendo sido homologada inicialmente em setembro de 2001 no Brasil. A NBR ISO/IEC 17799 é dividida em 11 macro controles: Política de Segurança da Informação, Segurança Organizacional, Gestão de Ativos, Segurança Física e do Ambiente, Gerenciamento de Operações e Comunicações, Controle de Acessos, Aquisição, Desenvolvimento e Manutenção de Sistemas da Informação, Gestão da Continuidade do Negócio, Gestão de incidentes de segurança da informação, Conformidade e, o mais relevante para o presente estudo, Segurança em Recursos Humanos.

[43] "Política, treinamento e conscientização em segurança", disponível em http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=434&pagecounter=0&idiom=0

[44] "Olhar para o próprio umbigo", disponível em http://www.modulo.com/empresa/site/modulo_interna_lernota.jsp?pidNota=352&pTipoNota=clipping&pMenuPai=5&pLinkMenu=abre_menu
Alvaro Teófilo é responsável pela área de Segurança de Informação do Banco Santander Banespa. Foi também Security Officer no Citigroup por 5 anos, atuando no Brasil e Estados Unidos, e também CSO do Grupo Caixa Seguros. É sócio-fundador da ISSA no Brasil (Information Systems Security Association), e foi professor-convidado do curso de MBA em Tecnologia da Informação da Fundace/USP e da Unieuro, em Brasília, onde lecionou o curso de Gestão de Segurança da Informação.

Ao se falar em conscientização não devemos somente focar no usuário final. Administradores e desenvolvedores de software padecem igualmente de falhas em sua percepção do que seja segurança.

Ao ser indagada de que forma a SBC – Sociedade Brasileira de Computação poderia contribuir para melhorar o cenário da segurança do espaço virtual brasileiro, Cristine Hoepers, analista de segurança do grupo de resposta a incidentes do Comitê Gestor da Internet (CGI) respondeu:

"A SBC pode incentivar a educação sobre o tema nos cursos de graduação das universidades, conscientizando os estudantes de que o profissional de Computação precisa se preocupar com segurança, que um desenvolvedor de software precisa criar um programa com o menor número possível de vulnerabilidades"[45].

Ainda segundo Hoepers, *"a redução do número de incidentes está relacionada com diversos fatores, todos relacionados com educação e conscientização de usuários e administradores de redes"*[46], acrescentando que usuários e administradores de sistemas devem ler os documentos preparados pelo grupo de resposta a incidentes do CGI, dentre eles "Práticas de Segurança para Administradores de Redes Internet" e "Cartilha de Segurança para Internet"[47].

Os executivos também deveriam ser alcançados por este processo de conscientização. Afinal de contas, as decisões acerca do volume de recursos a ser investido em segurança, e em que áreas, são tomadas por executivos que, a menos que estejam devidamente sensibilizados, podem investir pouco ou, talvez pior, muito numa área não prioritária, esquecendo-se do necessário investimento nos recursos humanos.

Em 2001 a NASA começou a criar um programa de treinamento em segurança em TI para capacitar todos os seus funcionários. Para o responsável pela proteção dos sistemas de informação da agência americana, Scott Santiago, *"mudar a mentalidade das pessoas que trabalham na organização será a melhor solução para garantir a segurança do órgão"*.

Um dos problemas levantados por Santiago é que a maioria dos usuários considera a segurança em TI um inconveniente e que a proteção das informações da NASA é tarefa exclusiva da área de

[45] http://www.cgi.br/infoteca/artigos/entrevista16.htm
[46] http://www.cert.br/docs/reportagens/2003/2003-07-11.html
[47] disponíveis respectivamente em http://www.nbso.nic.br/docs/seg-adm-redes/ e http://www.nbso.nic.br/docs/cartilha/

segurança. A conjugação destes dois fatores pode tornar qualquer medida de prevenção inútil. Para ele, *"precisamos fazer com que a questão faça parte do dia-a-dia de cada trabalhador"*[48].

Para finalizar, vale dizer que funcionários treinados e conscientes aumentam de forma considerável o chamado "raio de conhecimento", aumentado com ele a capacidade de resistência de se cair nas armadilhas do engenheiro social[49].

"ALFABETIZAÇÃO" (aquisição de conhecimentos básicos)

Conscientizado acerca do problema, como tratar dele ? Como saber operar os diversos equipamentos e softwares e, mais ainda, como utilizar de forma adequada os diversos controles de segurança que a empresa lhe entrega ? Como se comportar em situações desconhecidas ?

É necessário um mínimo de informação de segurança não só para se navegar na Internet como também para se lidar com documentos e dados aos quais se têm acesso no mundo corporativo.

É necessário então este processo de se "alfabetizar" os colaboradores com relação aos perigos, ameaças e vulnerabilidades aos quais ele estará sujeito. Exposto aos conceitos básicos, o colaborador adquirirá familiaridade com o meio digital.

Para citar somente um caso de vulto, a Ericsson Telecomunicações experimentou uma mudança na linha de seus negócios de meados para o final da década de 90. De sua competência inicial em telecomunicações, ela teve de começar a migrar também para o negócio de dados, ou Datacom.

Para capacitar seus funcionários, empreendeu um programa chamado de Competence Shift que, na época, envolveu não só o treinamento de seus funcionários como também o financiamento de computadores para eles. A iniciativa cobriu desde os executivos até colaboradores envolvidos em atividades estritamente ligadas à produção, com milhares de pessoas passando por treinamentos que, no Brasil, foram ministrados por professores de respeitadas universidades.

Quando se fala em conhecimentos básicos, dois conceitos podem ser aplicados:

[48] http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=7&objid=626&pagecounter=0&idiom=0

[49] "Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas Organizações", monografia de Mário César Pintaudi Peixoto disponível em http://www.modulo.com.br/pdf/contexto_da_vulnerabil.pdf. O autor lembra ainda que *"algumas autoridades recomendam que 40% do orçamento geral para segurança da empresa sejam aplicadas ao treinamento da conscientização"* (03. MITNICK, Kevin D.; SIMON, William L. A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Pearson Education, 2003.)

1. conhecimentos "simples": são aqueles que, sem dúvida alguma, deveriam ser ministrados a todos os usuários. Como funciona a Internet, o correio eletrônico, os certificados digitais, a criptografia, os ataques de engenharia social, endereços de IP etc, numa linguagem compreensível a eles. A partir destes conhecimentos outros poderiam ser adicionados em treinamentos mais avançados. Estes primeiros, porém, seriam a base, o "alfabeto" mínimo para se comunicar, compreender e ser compreendido.
2. conhecimentos "de base": são aqueles que os administradores de sistemas e desenvolvedores deveriam conhecer para poder melhor desenvolver, operar e configurar os diversos dispositivos de segurança que lhes são confiados. Falamos aqui dos diversos protocolos em uso na rede e de como alguns ataques se valem deles e de falhas em suas implementações para melhor ser propagarem.

O segundo tipo de conhecimento acima listado é freqüentemente esquecido. Muito treinamento de produto é ministrado. No entanto, não é bom saber como configurar um firewall para se proteger de um ataque do tipo *SYN flood* se o administrador não sabe o que seja um *SYN flood*.

TREINAMENTO

Neste *continuum* que é o processo de aprendizagem, o terceiro patamar (e não o último) é o treinamento.

Treinamento visa a aprimorar, a realizar com mais eficiência algo que já se sabe. Na definição de Marcus Vinicius Pereira, *"treinamento é uma atividade educacional focada na melhoria do desempenho, de forma a fazer melhor uma determinada tarefa"*[50].

Qual seria a diferença entre educação e treinamento ? Ouvi certa vez a seguinte distinção de um representante do SENAI do sul do Brasil:

"Se sua filha chegasse em casa e dissesse que teve uma aula de educação sexual na escola você acharia normal. Mas se ela chegasse e dissesse que teve um treinamento sexual na escola você ficaria preocupado"[51].

Treinamento, voltando a citar o artigo de Marcus Vinicius:

[50] " Desempenho turbinado", disponível em http://www.campogrande.news.com.br/debates/debates.htm?id=651

"(...) é sempre focado na prática e isso parece não estar claro para as empresas quando contratam ou programam essa atividade, assim como não é devidamente clara a importância dos esforços necessários que a mesma forneça os melhores resultados. No Brasil, o índice de horas treinamento por pessoa ao ano, apesar de apresentar-se em ascensão, ainda representa apenas 40% do tempo utilizado nos países desenvolvidos".

O treinamento é focado na prática e visa a ensinar não só como fazer mas também como fazer da melhor maneira.

Com o treinamento espera-se obter um melhor desempenho, desempenho este que pode ser medido para se saber se o treinamento foi eficaz ou não.

Vamos a um pequeno exemplo de como o treinamento expande as idéias lançadas na etapa anterior de "alfabetização" ou de "aquisição de conhecimentos básicos":

1. Ao se "alfabetizar" um usuário acerca de sessões seguras na Internet (o uso do protocolo SSL), pode-se dizer que se ele enxergar um cadeado (ou chave, dependendo do navegador de Internet) no canto inferior da tela, podem ser enviados dados sensíveis pela rede porque toda a sessão está sendo criptografada.
2. No treinamento, no entanto, deve-se ensinar que:
   a) Para ser seguro, ele deve digitar o endereço no navegador para se chegar à página desejada. Se ele clicar num link encontrado num e-mail ou numa página da Internet ele pode, eventualmente, pensar que está num site quando na verdade está em outro.
   b) Mesmo digitando o link, não há uma garantia de que ele esteja mesmo no site desejado se um vírus tiver alterado o arquivo hosts no Windows, de forma a redirecionar o usuário para um site diverso daquele que se pretendia.
   c) Para aumentar a certeza de que se está no site correto, pode-se clicar duas vezes no cadeado para se abrir o certificado digital do site. Este, diz-se, é seguro.

[51] Para os devidos créditos, Marcus Vinicius Pereira (e também Marc Rosemberg, especialista em e-learning – vide http://banners.noticiasdot.com/termometro/boletines/docs/elearning/elearning-brasil/2003/0103/elarning-brasil_enero2003_2.pdf) dão o mesmo exemplo para explicar a distinção entre educação e treinamento.

d) No entanto, pelo menos uma vulnerabilidade conhecida do Internet Explorer permitia que se visualizasse, digamos, o certificado de um banco conhecido quando, na verdade, o usuário estivesse visualizando um site falso[52].

Este é só um exemplo de como o capacidade de se precaver contra falhas de segurança pode ser aumentada através de treinamentos específicos.

EDUCAÇÃO

Poderíamos parar no terceiro patamar (o treinamento que aperfeiçoa) se a tecnologia e, consequentemente, o conhecimento fossem estáticos. Se ambos evoluem, no entanto, os perigos e ameaças também evoluem. E de forma incrivelmente rápida.

Para o filósofo Pierre Lévy:

"Toda e qualquer reflexão séria sobre o devir dos sistemas de educação e formação na cibercultura deve apoiar-se numa análise prévia da mutação contemporânea da relação com o saber. A esse respeito, a primeira constatação envolve a velocidade do surgimento e da renovação dos saberes e do know-how. Pela primeira vez na história da humanidade, a maioria das competências adquiridas por uma pessoa no começo de seu percurso profissional serão obsoletas no fim de sua carreira. A segunda constatação, fortemente ligada à primeira, concerne à nova natureza do trabalho, na qual a parte de transação de conhecimentos não pára de crescer. Trabalhar equivale cada vez mais a aprender, transmitir saberes e produzir conhecimentos"[53].

Treinamentos, desta forma, começam a ficar rapidamente obsoletos. A questão não é saber somente como fazer, mas saber como acontece para nos precaver quando acontecer de forma ligeiramente diversa.

Treinamentos automatizam nossa resposta, mas somos mais que autômatos. Respostas pavlovianas têm os animais. Por isto é que se diz que "você treina macacos mas pessoas, você educa".

[52] Vulnerabilidades deste tipo não são exclusividade do Internet Explorer. No artigo "Falsificación de firmas RSA y navegadores" disponível em http://www.kriptopolis.org/node/2905, certa vulnerabilidade que permite sejam tomadas como verdadeiras assinaturas digitais falsificadas é apontada como sendo encontrada no Firefox e no Opera, enquanto o IE é imune a ela.

[53] http://www.sescsp.org.br/sesc/Conferencias/subindex.cfm?Referencia=168&ID=29&ParamEnd=9. Pierre Lévy é autor de "Cibercultura" (Editora 34, 1999).

No final do processo de aprendizagem, o que se busca são pessoas educadas na Segurança da Informação.

Uma boa palavra em inglês que expressa esta idéia é *mindset*. Vejamos algumas definições para esta palavra:

- uma atitude fixa mental ou uma disposição que predetermina a resposta de uma pessoa a uma situação e suas interpretações dela.
- uma inclinação ou hábito
- uma atitude mental habitual ou característica que determina como se interpreta e se responde a situações

Numa interpretação (bem) livre da palavra, diria que *mindset* é "ter na veia". Ter *mindset* de segurança, neste contexto, é ter segurança "correndo nas veias". Os atos e atitudes de quem tem mindset de segurança são tão normais que passam despercebidos para ele.

Voltando ao gráfico da aprendizagem contínua (figura 7): ao se focar na educação como objetivo final o que se espera é ter indivíduos com alto nível cognitivo, com habilidades internalizadas, com capacidade para pesquisar, analisar, avaliar e julgar.

Especificamente falando dos administradores de sistemas e técnicos de TI, em um recente artigo disponibilizado na Network World[54] o autor enumera três tipos de treinamento que deveriam ser aplicados às equipes responsáveis pela segurança:

1. o treinamento específico para cada novo produto de software importante;
2. o treinamento sobre os conceitos de base e as idéias por trás das redes e segurança;
3. uma visão geral e uma sabedoria que somente vêm de um mentor com muita experiência ou através de um intensivo treinamento on-the-job. Ser capaz de ver o grande quadro com os requisitos do negócio e traduzi-los para uma política de segurança é algo que vem somente com prática e perspectiva. É o mais difícil de obter.

Este último "treinamento" é o que tentamos alcançar, um estágio de educação em que os responsáveis pela Segurança da Informação obtenham uma visão geral e uma "sabedoria" (capacidade de pesquisar, analisar, avaliar e julgar) .

[54] "The six worst security mistakes", disponível em http://www.networkworld.com/techinsider/2006/082806-guide-security-index.html?t5

Voltando aos usuários comuns, vejamos uma situação simples: o treinamento pode apontar diversas das técnicas de scam, em que um usuário recebe um e-mail com links que apontam para páginas falsas de bancos onde seus dados pessoais como conta-corrente e senha podem ser roubados. Se o usuário não for alertado para o problema maior da engenharia social, ele pode escapar do phishing mas cair num ataque de vishing ou smishing como os citados anteriormente. Ou mesmo clicar numa link criminoso plantando numa página legítima da Wikipedia[55]. Como se vê aqui, a questão é mais do que treinar para responder melhor, é educar para ser sensível a ataques que não puderam ser previstos ao tempo de um treinamento.

Tendo em vista também o crescimento exponencial do conhecimento e a entrada de um número cada vez maior de pessoas no mundo digital, faz-se necessário o investimento em educação não somente nos usuários enquanto funcionários, mas também dos jovens (futura força de trabalho), crianças (elas, as primeiras e mais inocentes vítimas da desinformação), pais (para orientar e monitorar seus filhos) e professores (como educadores e multiplicadores de conhecimento).

Iniciativas devem ser abertas para cobrir este amplo espectro de usuários, em suas diversas linguagens e em seus níveis heterogêneos de conhecimento.

Diversas empresas e organismos têm se dedicado a melhor educar seus usuários ou os usuários de Internet de um modo geral.

Dentre as várias iniciativas, merecem destaque:

- A Cartilha de Segurança para Internet do CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, com recomendações e dicas sobre como o usuário pode aumentar a sua segurança na Internet[56].
- O Site da Microsoft Brasil, que a partir de agosto de 2003 passou a melhor orientar os usuários de seus produtos com relação a boas práticas de segurança[57].
- A iniciativa Navegue Protegido, para pais, jovens e professores[58].

[55] Em novembro de 2006 cibercriminosos plantaram um artigo falso na Wikipedia alemã, discorrendo sobre uma falsa variante do vírus Blaster e disponibilizando um link para a solução do problema, link este que na verdade carregava um outro malware na máquina do usuário

[56] Disponível em http://cartilha.cert.br/, o documento apresenta o significado de diversos termos e conceitos utilizados na Internet e fornece uma série de procedimentos que visam melhorar a segurança de um computador.

[57] " Segurança", em http://www.microsoft.com/brasil/athome/security/default.mspx e, particularmente, o "Proteja seu PC", em http://www.microsoft.com/brasil/proteja/default.asp

[58] http://www.navegueprotegido.org/

- Bancos como o Banco do Brasil[59] e o Itaú, que recentemente lançou o Programa Mais Segurança[60].

Com uma educação contínua, o usuário (a primeira linha de defesa) estará preparado para, ainda que como elo mais fraco, realizar de forma mais eficiente a sua parte na corrente da Segurança da Informação.

[59] http://www.bb.com.br/appbb/portal/bb/ds2/index.jsp
[60] http://www.itau.com.br/campanhas/inst/seguranca/0607/mais_seguranca/hotsite_seguranca.htm. Outras dicas de segurança em http://www.itau.com.br/seguranca/home_seguranca.htm

OK, feito isto, por que ainda falhamos ?

A Peste (dirigindo-se à diretoria)*: Um intruso desconhecido recentemente invadiu nossa rede usando uma conta de super-usuário, o que deu a ele acesso a todo o sistema.*

Margo: Precisamente aquilo que você foi pago para evitar.

A Peste: Alguém não quis se chatear lendo meu memorando cuidadosamente preparado que versava sobre as senhas mais comumente usadas. Agora, como eu já meticulosamente indiquei, as quatro senhas mais usadas são AMOR, SEXO, SEGREDO e (olhando para Margo) *... DEUS. Então, Sua Santidade se incomodaria de mudar a sua senha?*

Diálogo em **Hackers – Piratas de Computador** (Hackers), 1995

Corria o ano de 1987 quando estive num CPD na cidade de Brasília para instalar um equipamento de análise de imagens de satélites. Ao ser perguntado sobre que cuidados deveriam ser tomados com relação àquele equipamento comentei somente que, por se tratar de um PC, os usuários deveriam se abster de beber próximo a ele (o derramar de um líqüido poderia danificar as placas internas) ou mesmo de fumar, já que partículas ainda que pequenas poderiam prejudicar o funcionamento dos discos rígidos.

O gerente da área então deu então um passo para trás, ofendido, dizendo que aquele era um ambiente de CPD e que os usuários já estavam habituados a estas recomendações, não sendo necessário sequer citá-las.

Na manhã seguinte, ao me aproximar do equipamento para os últimos testes, notei que havia um copo de café sobre ele e cinzas de cigarro sobre a cadeira ...

Ainda que este não seja um capítulo muito agradável de se ler, temos de tocar no assunto: as pessoas recusam-se a seguir determinadas orientações, ainda que cientes de suas possíveis conseqüências, muitas vezes por acreditarem que naquela situação não vai acontecer nada, já que tudo está sob o seu controle ...

Nossa opinião, no entanto, é de que estabelecidos os procedimentos, conscientizados/treinados/educados os funcionários, falhas cometidas de forma consciente deveriam ser punidas como danosas ao patrimônio da empresa e serviriam de exemplo (ainda que impopulares).

Os americanos têm um termo para isso: "carrot and stick policy" ou "política da cenoura e do porrete". Quando o conhecimento e a orientação são fornecidos e o comportamento dos funcionários deliberadamente contraria ambos não há educação que conserte, mas punição. A empresa tem de confiar em seus funcionários (a primeira linha de defesa). Se não confia que eles vão fazer o que se espera deles e para o que eles foram contratados, a hora é de trocar de colaboradores.

Alguns exemplos de comportamento que deveriam ser punidos ou reprimidos incluem:

- uso de e-mail para envio de correntes e pornografia
- uso indiscriminado da Internet
- liberação de acesso para outros
- fornecimento de senha particular a colegas
- instalação de software não permitido
- burlar quaisquer que sejam os mecanismos de segurança

Vamos a um exemplo recente acerca deste assunto: num experimento conduzido pelo The Training Camp em fevereiro de 2006[61], vários trabalhadores que estavam adentrando a cidade de Londres receberam CDs cujo conteúdo, dizia-se, continha uma promoção do Dia dos Namorados (Valentine's Day). Apesar das caixas com os CDs trazerem impresso um claro alerta sobre o fato de que instalar software de terceiros poderia significar quebras nas políticas de segurança das companhias, muitos trabalhadores instalaram tal software em seus PCs. Alguns destes trabalhadores eram empregados de conhecidas empresas de serviços financeiros. Os CDs não continham mais do que um código que informava ao The Training Camp quantos usuários haviam aberto os CDs. Mas poderia ter instalado software muito mais danoso.

[61] "Proof: Employees don't care about security", disponível em http://software.silicon.com/security/0,39024655,39156503,00.htm

Apesar da obviedade do comportamento inseguro dos usuários e totalmente contrário às políticas de segurança das empresas para as quais trabalhavam, Bruce Schneier, em seu weblog[62], adiciona alguns comentários instrutivos:

"Concluir que empregados não se importam acerca da segurança é um pouco ingênuo. Empregados se importam com a segurança; eles simplesmente não a entendem (...) [a] tecnologia muda rapidamente, e qualquer intuição que um empregado tenha ficará rapidamente obsoleta dentro de um curto período de tempo.

"Educação é uma maneira de lidar com isto, mas educação tem suas limitações (...) Punição é uma outra forma de educação, e meu palpite é que seria mais efetivo. Se os bancos demitissem todos que caíram no truque do CD-ROM-na-rua, você pode apostar que ninguém faria isto novamente (ao menos, até que todos esquecessem). Isto nunca aconteceria, no entanto, por que os efeitos morais seriam enormes.

"Mais que culpar este tipo de comportamento dos usuários, nós estaríamos melhor servidos se focássemos na tecnologia. Por que um usuário médio de computador num banco precisa ser capaz de instalar software de um CD-ROM ? Por que não bloquear esta ação pelo próprio computador, ou pelo menos informar o departamento de TI ? Computadores precisam ser seguros independente de quem está sentado em frente deles, não importa o que eles façam".

Novamente, Schneier tenta mover o eixo da discussão para a tecnologia, reconhecendo que usuários não compreendem totalmente todos os aspectos da segurança. Neste caso em particular, ela seria de valia, mas não em todos aqueles mostrados no Jogo da Segurança do capítulo anterior.

Se não podemos resolver tudo com tecnologia, o que fazer ? Voltando aos segundo parágrafo do comentário de Schneier, vemos que:

1. educação pode trabalhar a favor, com mais campanhas de conscientização;
2. quando, a despeito disto, os funcionários erram, alguma forma de punição (outro tipo de educação) deveria ser empregado.

Comentando o ocorrido no fórum de notícias da Silicon.com, um usuário anônimo sugere que para se obter um completo comprometimento de seus colaboradores, é necessário ter uma política de segurança corporativa e enfatizá-la. Funcionários que desprezam tal política deveriam ser demitidos, enquanto que funcionários que relatam suspeitas de quebras (ou quebras reais) de

[62] " Alguém acha que este experimento teria um resultado diferente?", disponível em http://www.schneier.com/blog/archives/2006/02/proof_that_empl.html

segurança deveriam ser recompensados. Os contratos individuais de trabalho deveriam trazer como anexos a Política de Segurança e um termo de responsabilidade em seguir tal política[63].

Já Nell Walton, comentando no weblog de Schneier a opinião deste acerca do experimento da The Training Camp, tenta uma outra abordagem: sugere obter a colaboração daqueles que infringiram as políticas de segurança, fazendo-os serem entrevistados por uma autoridade de fora da empresa que enfatizaria a questão das responsabilidades individuais no caso (quem não se intimidaria com a possibilidade de ser enquadrado como suspeito numa investigação criminal de quebra de segurança ?). Poderiam, assim, partir deles algumas sugestões de como evitar isto no futuro, tornando-se eles mesmos os multiplicadores das novas estratégias para seus companheiros de trabalho[64].

O importante a notar é que se somente a tecnologia não pode evitar quebras de segurança e se todo o necessário já foi feito na área da educação (incluindo conscientização e treinamento), algo deve ser feito de forma complementar, seja punindo, seja obtendo a colaboração dos que erraram no sentido de se fortalecer os mecanismos de segurança já existentes.

A educação é o foco, obter o compromisso dos usuários em trabalhar de acordo com ela é o alvo.

[63] http://software.silicon.com/security/0,3800003029,39156503,00.htm?PROCESS=show&ID=20063925&AT=39156503
[64] http://www.schneier.com/blog/archives/2006/02/proof_that_empl.html, comentário enviado por Nell Walton em 20 de fevereiro de 2006

Bibliografia

Rick: Você tem certeza de que deve ficar brincando com esta coisa ?
Evelyn: É apenas um livro. Nunca alguém se machucou só de ler um livro.

Evelyn respondendo a Rick, momentos antes de ler o encantamento no Livro dos Mortos que ressuscitou Imhotep, em **A Múmia** (The Mummy), 1999

SCHNEIER, Bruce. **Segredos e mentiras sobre a proteção na vida digital**. Rio de Janeiro: Campus, 2001

GARFINKEL, Simson e SPAFFORD, Gene. **Comércio & Segurança na Web**. São Paulo: Market Press, 1999

WURMAN, Richard Saul. **Ansiedade de informação – Como transformar informação em compreensão**. São Paulo: Cultura, 1991

Ao longo do trabalho diversos links de Internet foram apresentados em notas de rodapé, motivo pelo qual nos abstemos de reproduzi-los aqui.