H2HC

StaySafe

Isto sim é informação de qualidade !!!

3ª Edição

www.staysafepodcast.com.br

Setembro - 2010

Editorial

Sejam Bem Vindos a nossa 3ª Edição da Revista H2HC Stay Safe.

União da Revista Stay Safe com a Hackers to Hackers Conference (H2HC)

É com enorme satisfação que anunciamos a união da Revista Stay Safe com a Hackers to Hackers Conference (H2HC).

A H2HC é considerada atualmente uma das principais conferências nacionais em relação ao desenvolvimento e a pesquisa na área de segurança da informação. (www.h2hc.com.br)

Acreditamos que esta união só tende a agregar maiores conhecimentos aos nossos leitores e ressaltar cada vez mais a importância de se considerar a segurança da informação uma área vital para o desenvolvimento de um negócio sustentável.

A H2HC e a Stay Safe estão juntas nestas iniciativa de prover a Segurança da Informação, porém vale lembrar que diferentemente da conferência, a revista não exige em sua publicação a necessidade de um profundo nível técnico em seus artigos, dando assim oportunidade para expressão sobre qualquer assunto relacionado a segurança da informação para diferentes públicos.

Boa Leitura e Divertimento!!

Equipe H2HC Stay Safe
Filipe Balestra
Jordan M. Bonagura
Rodrigo Rubira
Thiago Bordini

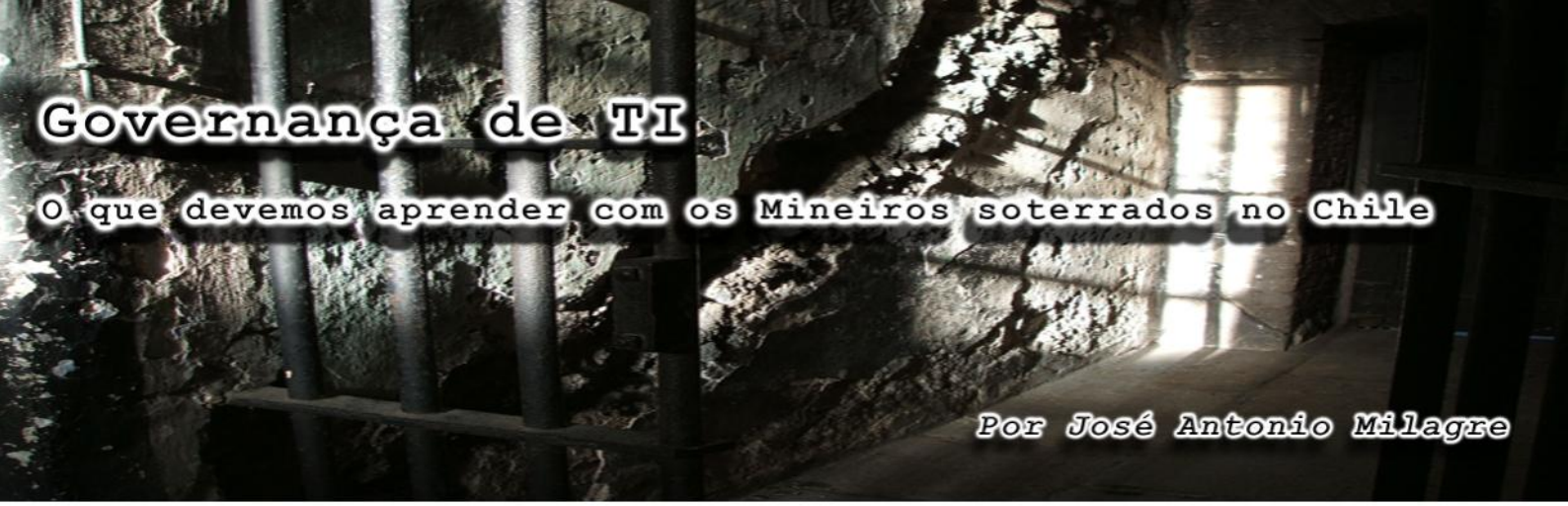
H2HC
Hackers to Hackers Conference

Fale com a Revista H2HC Stay Safe
contato@staysafepodcast.com.br

Índice

H2HC StaySafe

REVISTA H2HC STAYSAFE
CALL FOR PAPERS
cfp@staysafepodcas.com.br



Governança de TI

O que devemos aprender com os Mineiros soterrados no Chile

Por José Antonio Milagre

"Estamos todos bem no refúgio, os 33".

Relato dos mineiros após duas semanas do incidente, quando foram encontrados.

A perplexidade envolvendo soterramento dos 33 mineiros chilenos, em agosto de 2010, presos a 700 metros de profundidade, em uma câmera de segurança (com 50 metros quadrados) da mina de São José não se limita pela tragédia propriamente dita. Mais do que preocupação pela vida destas pessoas, fato que nos faz refletir é o exemplo e aprendizado que o episódio nos apresenta, os quais podemos aplicar com precisão em muitos projetos profissionais e corporativos, principalmente em tecnologia da informação. Diversos institutos fundamentais ao êxito de estratégia, projetos, segurança da informação e operações são aclarados quando refletimos sobre como estas pessoas estão lidando com o imprevisto, os quais apresentamos:

1) Auto-Conhecimento

Assim como na mina, mas como em qualquer negócio, sobretudo na área de tecnologia da informação, é indispensável que os envolvidos conheçam bem as carcterísticas do negócio em que atuam. Todo gestor deve ter um mapa de cada processo, sobretudo para que este processo atenda as necessidades do negócio, como cultura, políticas, condições sociais, políticas, geográficas e outras características do negócio. Auto-conhecimento também permite que em operações cada recurso empregado nas atividades corporativas tenham um conjunto de habilidades necessárias. No caso dos mineiros, todos eram cientes dos detalhes mais íntimos desta atividade, bem como conheciam claramente as habilidades de cada um dos integrantes do grupo, consequentemente, concebendo um mapeamento prévio dos recursos à disposição e principalmente, como e quando utilizá-los, em caso de um incidente como o que experimentaram.

2) Análise de Risco

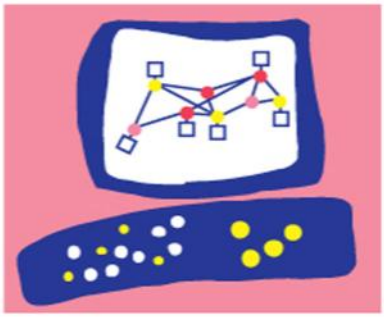
Justamente por conhecerem absolutamente o negócio que operam os mineiros puderam criar uma análise de risco, onde puderam compreender, as vulnerabilidades existentes na operação, as ameaças que atuam sobre estas vulnerabilidades, e principalmente a probabilidade de incidentes ocorrerem. Conhecendo tais fatores, os mineiros conseguiram avaliar o impacto dos riscos e consequentemente, a urgência e prioridade em tratá-los. Com isso, sabendo das condições climáticas do terreno e dos constantes deslocamentos de terras, desenvolveram uma "câmera de segurança", prevendo a hipótese de um incidente desta natureza. Só estão vivos graças a esta análise, que lhe deram informações para decidirem implementar medidas de contingência e abrigo. No ITIL, a análise de risco está no âmbito do gerenciamento da continuidade.

3) Resposta a incidentes

Se os chilenos soterrados não tivessem capacitação para responderem a incidentes desta natureza, com certeza já estariam mortos. Isto fez toda a diferença para eles, e isto faz toda a diferença no seu negócio. Infelizmente, empresas que atuam de forma reativa e não pró-ativa, tendem a perder as rédeas quando um incidente acontece, onde excepcionalmente o resultado é catastrófico. No caso dos mineiros, cada integrante investiu-se da qualidade de um recurso para uma atividade de um processo, cujo objetivo imediato é devolvê-los ao convívio de seus familiares, logicamente, com a preservação da vida. Logo, se arrumaram com uma "solução de contorno", onde buscaram estabelecer uma convivência que primasse pela estabilidade mental, saúde, organização. Não bastasse, realizaram um excelente atendimento ao incidente em primeiro nível, onde muniram de informações as equipes de resgate que estão na superfície, informações estas que foram importantes para definir a melhor alimentação, ventilação, apoio psicológico e principalmente, serviu de insumo para que as equipes de resgate criassem a melhor estratégia para recuperação, com o objetivo de salvar todas as vidas e impedir a desestabilização mental, com consequente depressão. No caso apresentado, se a equipe de segundo nível do incidente, que são os resgatadores que estão na superfície, não tiverem condições para o regaste, deveriam recorrer ao outsourcing ou a terceiros. E assim foi feito eis que a NASA foi chamada para auxiliar à resolução do problema.

4) Plano de contingência e recuperação do desastre

Se eu armazeno históricos de incidentes eu consigo ter "base de situações passadas ou erros conhecidos" e consequentemente me preparar para ao futuro, prevendo ações corretivas e sabendo como agir caso a história se repita. Posso saber que no verão, o risco de deslocamentos de terra é maior, razão pela qual precisarei de estratégias assertivas para que este evento futuro e incerto seja repudiado ou no mínimo tratado.
Crio então um plano de contingência, onde defino como deverá ser a comunicação, apoio e operação durante um incidente. Na mina uma fenda com 7 centímetros de diâmetro foi aberta e por ela é que todo o suporte aos mineiros está sendo realizada. Uma decisão acertada e tomada no tempo adequado, certamente fruto do estudo de casos passados semelhantes. Os mineiros foram muito perspicazes em definirem os critérios para ativação do plano de contingência, onde rapidamente desenvolveram os arranjos recíprocos, planos de fortificação (como o pôster da mulher pelada e o jogo de dominó), bem como os responsáveis por colocar em prática cada atividade do plano, com vistas ao objetivo maior: A manutenção da vida, seja a alimentação, a abordagem psicológica, a ventilação, etc. Plano de recuperação de desastres também envolve plano "B", em caso do impedimento dos planos prioritários, como no caso da mina, onde o duto de ventilação poderá ser alargado para servir de resgate.



5) A liderança

Os mineiros podem nem saber a teoria, mas governança (de tecnologia) nada mais é do que o desafio como aplicar liderança, estrutura e processos para que a ti atinja os objetivos de negócios (governança corporativa). Onde temos muitas pessoas envolvidas, sobretudo no tratamento de um incidente catastrófico, é preciso que tenhamos uma matriz de responsabilidades clara e definida, em Governança chamada de matriz RACI (Responsible, Accountable, Consult and Inform), também muito utilizada em projetos. Igualmente, não existe operação ou projeto sem liderança, que pode envolver uma ação, uma mudança ou mesmo a comunicação. Na mina, acertadamente, surgiram as figuras dos líderes, como o religioso e o de comunicação com imprensa. O papel do líder, aqui, é coordenar as atividades e transmitir as necessidades dos mineiros. Na TI não é diferente, onde o líder deve estar em sintonia com a área de negócios e principalmente sensibilizá-la sobre a necessidade de novos processos visando um melhor alinhamento da TI ao negócio. O Líder é o que abraça a causa e define a estratégia de engajamento, cria o "report" e faz com que todos os recursos sejam conjugados para um objetivo comum. Tal ponto foi fundamental para a sobrevida dos mineiros soterrados no Chile.

Conclusões

Tal episódio demonstra claramente que só teoria não é suficiente para que operações, projetos e resposta a incidentes sejam efetivas. A despeito dos catedráticos e amantes da doutrina, o exemplo vem de mineiros, que absolutamente preparados de fato, estão lidando com um incidente grave com absoluta governança e controle, com excelente relacionamento com todos os envolvidos no projeto de resgate. Efetivamente que nada é fácil e o resgate lida com premissas e fatores desconhecidos. Apesar disso, deve-se destacar que a postura destas pessoas tem cooperado contundentemente para ampliar suas chances de sobrevivência. Evidentemente que lições serão tiradas deste fato, e deverão, servir de base para a melhoria contínua de tais serviços, assim como na Governança, onde o alinhamento da ti com o negócio pressupõe o aperfeiçoamento dos serviços (Ciclo de Demming, PDCA), sobretudo, convergindo para que incidentes não mais ocorram, e caso ocorram, sejam rapidamente contingenciados e solucionados em nível temporal aceitável, impedindo o advento do dano, em uma dinâmica constante de "aprender com o erro".

José Antonio Milagre

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

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

Mundo IDS - "Projeto de Regras para o Snort para detecção de Malwares Made in Brasil"

Já faz muito tempo que temos a idéia de criar o projeto malwares-br na comunidade snort-br, mas por diversos motivos, em especial a falta de tempo, nunca chegamos a iniciamos o projeto. Em uma conversa no final de setembro chegamos a uma conclusão: "Se formos aguardar tempo livre para iniciar, este projeto nunca sairá de uma boa idéia". Com isso demos início ao projeto, lançando a idéia em diversos locais, como twitter e listas, criando também um blog para acompanhamento.

O endereço do blog é o http://malwaresbr.blogspot.com onde postaremos as análises para que todos possam ter acesso e, o mais importante, contribuir reportando falso-positivos e negativos, bem como sugerir melhorias, visto que disponibilizaremos os pcap's também além das rules.

O foco principal do projeto é a criação de regras que detectem comunicação/infecção de máquinas pelos nossos malwares brasileiros, estes que na sua maioria são bankers. A grande idéia é de poder colaborar na proteção com a internacionalização de malwares que estão sendo cada vez mais focado, como, por exemplo, o Stuxnet . Antigamente os ataques eram mais genéricos/abrangetes, já atualmente este cenário está totalmente modificado, pois podemos ver muitos malwares específicos para, por exemplo, Itaú , Banco do Brasil , Bradesco , operadoras de cartões, dentre outras formas financeiras, e isto move o desenvolvimento desses artefatos.

Para fazer parte do projeto você não precisa ser nenhum expert em snort, análise de malwares e escrita de regras, o mais importante é ter comprometimento e dedicar parte do seu tempo livre para contribuir, estamos bem dispostos a compartilhar informação e ajudar profissionais iniciantes a conhecer o prazer dessa "brincadeira".

Inicialmente além do tempo acima citado estamos buscando constantes parcerias com fontes de arquivos maliciosos, mas estamos bem encaminhados, pois a grande maioria tem interesse nessa proteção extra, justificada especialmente pelo prejuízo que esses malwares Made in Brasil causam.

Caso você tenha interesse em participar deste nosso projeto, existe inúmeras maneiras de contribuir e com certeza qualquer uma será muito bem vinda.

Algumas das formas de ajudar que posso listar são:

- Envio de link de malwares;
- Criação de regras baseado em pcap de sandboxes;
- Testes das regras usando em seus ambientes e
- Tunning de regras feita por outros.

Vamos tocar o projeto, ganhar mais adeptos e quem sabe virar uma categoria no Emerging-threats ou uma referência em regras para Snort e Clamav para as nossas ameaças nacionais.

Para acompanhar:

http://malwaresbr.blogspot.com

http://www.snort.org.br

Happy Snorting!

Rodrigo Montoro
Twitter: @spookerlabs

Rodrigo Montoro (Sp0oKeR)

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.

Tratamento de Incidentes de Rede

Por Márcio Marchy

1. Introdução

A popularização das redes de computadores e a necessária integração entre elas trazem consigo um grande número de aplicações distribuídas disponíveis aos usuários nas redes corporativas e na própria Internet. Simultaneamente ao aumento dos sistemas distribuídos tem se verificado um número substancial de incidentes de rede.
Neste contexto, o tratamento de incidentes de rede vem adquirindo importância cada vez maior em qualquer organização, tendo em vista os prejuízos decorrentes de um incidente, seja a invasão de um site, o comprometimento de uma aplicação, o furto de informações corporativas, o acesso a dados sigilosos, e até mesmo o abalo na imagem ou marca da instituição afetada, que pode trazer custos difíceis de mensurar.
Neste breve artigo serão abordados os principais conceitos relacionados aos incidentes de rede e seu tratamento.

2. Incidentes de rede

Atualmente, tanto no meio acadêmico como no setores público e privado, um incidente é referenciado em sentido mais amplo como qualquer situação que possa resultar em um impacto significativo a um processo de negócio. O nível gerencial de qualquer instituição precisa entender o dano ou o custo associado caso algum processo de seu negócio seja atrasado, diminuído ou totalmente parado na eventual ocorrência de um incidente, seja um fenômeno natural, um erro humano, uma falha de software ou hardware ou um ataque direcionado [1].
Em um sentido mais restrito, direcionado à tecnologia da informação, um incidente de rede pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou às redes de computadores, ou seja, qualquer tentativa ou violação concreta de um sistema computacional [2].
Os incidentes de rede estão relacionados à violação de uma política de segurança, que define o que pode e o que não pode ser feito em uma instituição. Estas regras de utilização dos recursos são violadas quando pelo menos um dos três pilares da segurança da informação é afetado: a confidencialidade, a integridade ou a disponibilidade.
Confidencialidade diz respeito à utilização da informação somente por aqueles indivíduos que possuam este direito de acesso, prevenindo o acesso não-autorizado. O nível de confidencialidade deve ser mantido em todas as situações, seja no acesso ao dado armazenado em qualquer dispositivo, na sua transmissão através de um meio físico e no momento em que atinge seu destino.
Integridade é a garantia de que qualquer informação não seja modificada de forma não-autorizada, seja de forma acidental ou intencional. O desafio deste requisito é sempre manter a informação no estado em que os usuários esperam, sem qualquer modificação, durante o seu armazenamento ou transmissão.Por último, a disponibilidade deve garantir que a informação esteja acessível ao usuário sempre que o mesmo deseje ou necessite utilizá-la. Os sistemas e redes devem prover uma capacidade adequada que permita a execução e tráfego de dados de uma maneira previsível e com um nível aceitável de desempenho [3].
Alguns exemplos de incidentes de rede podem ilustrar os conceitos apresentados: um funcionário que forneça informações sigilosas da empresa ao concorrente caracteriza uma violação da confidencialidade; a alteração do site da corporação ou de informações de um banco de dados por um atacante viola a integridade desta informação; já a proliferação de um vírus na rede da instituição, o qual impossibilite o uso das estações de trabalho pelos funcionários exemplifica a violação do conceito de disponibilidade.

3. Tratamento de incidentes de rede

O tratamento de incidentes de rede é parte vital de qualquer ambiente de tecnologia da informação que pretenda ser bem-sucedido mas, frequentemente, é ignorado até que uma emergência ocorra e resulte em altos custos para remediar o problema, sem mencionar o possível abalo na imagem da instituição afetada e o stress gerado no pessoal envolvido nestes momentos de crise [1].

A bibliografia especializada da área é unânime em afirmar a necessidade de uma análise de riscos na instituição que permita avaliar o custo-benefício do estabelecimento de uma equipe de tratamento de incidentes. Esta análise fornecerá o nível de risco que a instituição está disposta a aceitar envolvendo seus principais ativos e processos de negócio. Baseada na avaliação de riscos, a alta direção pode decidir que não é vantajoso implantar medidas de segurança que diminuam a probabilidade de vulnerabilidades serem exploradas por qualquer tipo de ameaça.

O tratamento de incidentes de rede pressupõe a existência de algumas características básicas e a partir da decisão da alta direção, citada anteriormente, advém a primeira delas: possuir uma relação custo-benefício vantajosa para a empresa. Os investimentos nesta área somente serão realizados caso a ocorrência de incidentes de rede traga mais prejuízos do que a manutenção de uma equipe direcionada para esta atividade [1].

A segunda característica pressupõe que suas missões sejam voltadas para o negócio da instituição, de forma organizada e metódica. O tratamento de incidentes deve ser realizado da mesma forma que qualquer outro processo, com procedimentos e responsabilidades bem definidos. A terceira característica exige que a execução dos procedimentos seja eficiente, sem retrabalho ou duplicação de tarefas e que o tempo de resposta seja o mais rápido possível, evitando períodos de indisponibilidade e, novamente, causando o mínimo de prejuízos para a instituição.

Outras duas características que fecham o rol de atributos do tratamento de incidentes de rede são: a capacidade de repetição, ou seja, o procedimento de resposta à uma invasão de rede será o mesmo para diferentes empresas ou diferentes servidores que tenham sido invadidos, criando um padrão de tratamento dos incidentes que permitirá maior agilidade no processo de recuperação do alvo atingido; e a previsibilidade, na qual a alta direção ou a gerência precisa saber exatamente o que esperar do time de resposta para não ser surpreendida na eventual ocorrência de um incidente.

Além das características básicas citadas acima, pode-se enumerar uma série de atividades voltadas ao tratamento de incidentes de rede:

• Prevenção: apesar de parecer contraditório, a primeira atividade do tratamento de incidentes é justamente tentar evitar que os mesmos aconteçam, mantendo um comportamento proativo, através da análise e avaliação de riscos, monitoramento dos ativos e processos críticos do negócio, treinamento e conscientização em todos os níveis, definição de políticas de uso aceitável dos recursos de tecnologia da informação e aplicação das melhores práticas de segurança da informação;

• Planejamento: é considerada uma das mais importantes atividades, pois é a base que garantirá a eficiente execução dos próximos passos; inclui o completo entendimento dos papéis e responsabilidades de cada indivíduo envolvido com o tratamento de incidentes, treinamento adequado e documentação de políticas, normas e procedimentos;

• Detecção: a habilidade de uma equipe em tratar incidentes torna-se inútil caso não haja mecanismos de detecção e notificação que realmente funcionem; estes mecanismos podem ser automatizados com o uso de sistemas de detecção de intrusão e de notificação por usuários treinados que saibam agir e exatamente o que fazer ao verificar a existência de um incidente;

TREND MICRO™

• Análise: o entendimento do que ocorreu ou está ocorrendo é fundamental para que se desenvolva uma linha de ação de forma rápida; a natureza técnica de um incidente corrobora a necessidade de treinamento especializado citada na atividade de planejamento;

• Contenção: a contenção dos dados é executada fundamentalmente para proteger ou restaurar as funções normais do ativo ou negócio envolvido;

• Investigação: em algumas situações uma investigação formal pode ser necessária, o que pode envolver ações cíveis ou criminais, e mais uma vez é ressaltada a necessidade de conhecimento especializado para realização de perícia forense ou coleta de evidências que podem ser usadas na forma da lei;

• Erradicação: envolve a restauração do ativo a uma situação segura e operacional novamente, porém dependendo da gravidade do incidente pode ser necessário reconstruir todo um sistema desde o início ou adquirir novos equipamentos para que a evidência não seja comprometida;

• Postmortem ou análise pós-ação: uma vez que o problema tenha sido resolvido com sucesso, a equipe precisa revisar o que aconteceu e porquê, documentar o que foi observado e feito para que não venha a acontecer novamente ou para que novos procedimentos possam prevenir incidentes relacionados a este no futuro.

4. Conclusão

A dependência cada vez maior das redes de computadores e de sistemas distribuídos em todas as organizações traz consigo o aumento significativo dos incidentes de rede. Da mesma forma, o tratamento destes incidentes exige a formação de grupos especializados em segurança da informação com o objetivo principal de evitar prejuízos e garantir a disponibilidade, integridade e confidencialidade dos dados, serviços e equipamentos.

5. Referências bibliográficas

[1] WYK, Kenneth R. van; FORNO, Richard. Incident Response. United States of America: O'Reilly: 2001.

[2] HOEPERS, Cristine; OBELHEIRO, Rafael. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em <http://www.cert.br/certcc/csirts/csirt_faq-br.html> 2004. Acesso em 04 ago 2009.

[3] HARRIS, Shon. CISSP All-in-one Exame Guide. 4. ed. Estados Unidos da América: McGraw Hill, 2007.

Márcio Marchy

Tecnólogo em Processamento de Dados - Unisinos/RS;

Especialista em Redes de Computadores e Aplicações Internet - Unisinos/RS

Possui certificações MCSO e CISSP;

18 anos de experiência na área de TI;

Atua com Segurança da Informação desde 2001;

Atualmente trabalha em um CSIRT do setor público.

Uso das Redes Sociais nas Empresas

Por Gilberto Sudré

Parece que as redes sociais estão por toda parte. Todo dia uma nova rede surge para atender a um nicho específico de mercado, seja moda, finanças, amizade, culinária, compras e muitos outros temas.

É certo que estes espaços permitem uma grande interação entre seus participantes criando um ponto de encontro entre pessoas com interesses em comum. Este ambiente poderia ser muito bem utilizado por uma empresa que atua diretamente ou tem algum relacionamento com um mercado específico. Poder falar e ouvir sugestões e críticas de um publico interessado é tudo que uma empresa gostaria. Ao que parece poucas acordaram para isto.

Em geral observo que as empresas apresentam alguns comportamentos em comum em relação as redes sociais. Começando por empresas que se se escondem e fazem de conta que as redes sociais não existem. Esta certamente é a pior situação pois querendo ou não, as empresas já estão na redes sociais através da opinião (positiva ou negativa) de seus clientes.

Algumas empresas reconhecem a existência das redes sociais mas atuam como se fosse algo que acontece apenas fora de seus muros e não tivessem nada a ver com isto. Outras, além de reconhecer a existência das redes sociais permitem que alguns poucos colaboradores privilegiados tenham acesso a elas mas de forma limitada e controlada.

Realmente muito poucas empresas entendem, ou procuram entender, este novo ambiente e usam as redes sociais como um meio de comunicação com seus clientes, fornecedores e parceiros.

Este é um terreno novo que envolve muitos detalhes a serem avaliados e é normal que cada ambiente corporativo encare esta questão de forma diferente. Por isto é importante que as empresas definam claramente para seus colaboradores, através de políticas e procedimentos, quais são suas responsabilidades quando participando das mídias sociais e o que espera de sua atuação nestes locais.

Aprender como usar corretamente algo novo é muito importante. Por isto a capacitação dos colaboradores sobre o uso adequado de mídias sociais faz muita diferença no resultado final.

A empresa também deve monitorar as atividades de seus colaboradores, principalmente quando falam em nome da corporação, e entrar em ação quando identificar atividades inapropriadas

As redes sociais são ótimos espaços para que as empresas possam falar e principalmente ouvir seus consumidores. Por isto não devem ser desprezadas.

Gilberto Sudré

Consultor em Segurança da Informação;
Comentarista de Tecnologia da Rádio CBN;
Articulista do Jornal A Gazeta e Portal iMasters;
Redator e apresentador do quadro Tecnodicas na TV Gazeta;
Palestrante sobre Segurança da Informação, privacidade e infra-estrutura de redes.
Professor de Graduação e Pós-Graduação;
Instrutor da Academia Cisco;
Membro do comitê técnico CB21/CE27 da ABNT sobre Segurança da Informação;
Coordenador do ISSA Brasil – ES.
Co-Autor do livro "Internet: O Encontro de 2 Mundos";
Autor dos livros "Antenado na Tecnologia" e "Rede de Computadores".

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

16 anos do Início da Cena Hacker

Por Derneval da Cunha

Para aqueles que não se lembram de mim, eu sou o cara que escreveu o fanzine Barata Elétrica.
Quem só le a "2600 - Hacker Quaterly", bom, pode checar no "hacking in Brazil" e "Starting a hacker scene", etc.. Não sou o cara que começou a escrever textos do tipo que dão aos brasileiros a fama de serem os maiores web-defacers do mundo. Nada disso. Sou o cara que primeiro começou a escrever séria e continuamente sobre ética hacker, sobre o tipo "hacker" (que não precisa ser invasor de sites), sobre vírus de computador (quando os artigos decentes sobre o assunto na imprensa escrita eram raros e espaçados), sobre conferências de segurança informática e folclore de computadores, etc..

Meu trabalhão era acompanhar a discussão entre escolas do nível básico através da Internet. Aí soube deste "Hacker and Virus Congress" em Buenos Aires, Argentina. Cerca de 4 dias que eu usei para aprender e falar com gente da (agora extinta) revista HackTic, 2600 – Hacker Quaterly e vários
argentinos ligados a segurança informática, entre outras coisas.

Naquele tempo, pouca gente na América do Sul tinha contas na Internet (eu tinha várias, como 1807880@cat, rodrigde@spider, deus@qualquercoisa, etc..

Ganhava para fazer o trabalho que hoje as-pessoas fazem com o google). A maioria da cena “underground” acontecia em BBS, Fidonet ou coisas do gênero. O principal assunto de segurança era vírus de computador. Gerava um bocado de cobertura na Imprensa daqueles dias.

Muito difícil conseguir qualquer info sobre “assuntos proibidos”. No meu caso, tive que “conseguir” uma conta Internet acadêmica. Legalmente. Minha.

Não vou falar sobre conexões horríveis, sobre modens que não funcionavam legal (como é que era o nome, zoltrix? Bom, escrevi sobre isso para 2600-Hacker Quaterly - "Brazilian Phone system"). Estou falando de gente usando 600 bps ou 1200 bps, de vez em quando 2400 bps. Para baixar grandes arquivos de uma BBS a pessoa is preferir escolher online e depois ir à BBS em pessoa para pegar o material (No meu caso, nunca tive que usar telefone para nada, só usava Internet na universidade). Estudantes da segunda maior universidade da América Latina eram ignorantes sobre o assunto, exceto o que havia em filmes como "Wargames" (dizem que filmaram de novo e ficou uma porcaria). Esses foram os “anos dourados”.

Qual era o meu objetivo, então? Juntar gente, para trocar informação. Precisava de ter gente com quem conversar. E essas pessoas tinham que saber sobre "hacking". Tinha que espalhar a palavra, para conseguir isso. De forma que pessoas em todo o Brasil (aqueles que mereciam ser chamados de "hacker") poderiam saber sobre o que se tratava e fazer encontros.

Mais tarde, a coisa seria preparar para uma conferência hacker brasileira. De forma que eu comecei da forma mais fácil: através de uma publicação eletrônica (o termo mais usado seria e-zine ou fanzine eletrônico). Exatamente quando as pessoas estavam começando a aprender sobre a Internet. Não havia acesso comercial, só acesso acadêmico (pós-graduandos de universidades conectadas). Meu fanzine eletrônico foi o primeiro. O primeiro (e único, durante um bom tempo).

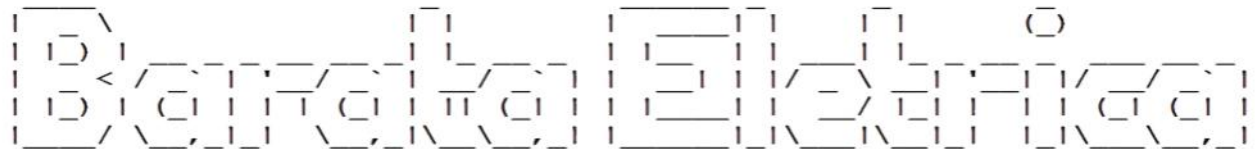
Meu chefe (na época) não me despediu quando soube dos meus planos. Ele entendia das coisas. Mas ao contrário do que ouvi falar sobre isto de fazer fanzine, sempre foi um grupo de pessoas que se juntou e fez. Eu estava sozinho. Tinha que me virar. Para fazer um e-zine, pedi permissão para publicar isto ou aquilo, "emprestei" arquivos em domínio público, copiei só pedaços de artigos ou, em vários casos, reescrevi do meu jeito.
Tem material que era tão bom que ainda está sendo publicado hoje (sem minha aprovação ou referência a minha autoria). A pior parte é que alguns autores que usaram textos inteiros foram best-sellers. Mesmo passados todos esses anos, ainda não estou 100% certo de que vou processar ou não este pessoal (*).

Tudo funcionou bem. Minha escolha de escrever (o fanzine) em ASCII puro ajudou a ser baixado e distribuido em BBSes pelo pais afora e no exterior, em lugares de língua portuguesa como Portugal e Moçambique. O fanzine Barata Elétrica se espalhou que nem praga. Apareceu em lugares como a Usenet, na lista 2600 e na soc.culture.brazil. Que eu mesmo coloquei para baixar foi na EFF e no etext.org (checar no Google para o URL atual ou acessem http://barataeletrica.cjb.net).

Gente da faculdade de Ciência de Computação da UFSC permitiu a existência de um "mirror" com os números do fanzine lá no website por cerca de 10 anos (agradeço a eles, com certeza). Na minha própria universidade, a USP, não queriam nem ouvir falar (eles me odiavam quase abertamente, uma vez o pessoal de informática me suspendeu o acesso Internet por mais de 2 meses).

Em pouco tempo, as pessoas começaram a escrever outras publicações, mais agressivas, como o ezine Axur 05, Nethack e uns outros, a maioria em BBS (1).

Era o tempo da prisão do Kevin Mitnick. Se alguém quisesse ser conhecido como um "hacker", ele e seus amigos escreveriam um Ezine. Montes de informação "boa" começaram a aparecer, ex: arquivos sobre o sistema telefônico brasileiro e como fazer chamadas gratuitas (já arrumaram esse problema).



O fanzine começou a ficar complexo. Descobri que gostava de escrever. Ficou sendo mais do que um hobby. Sempre levava mais tempo para escrever tudo. E se eu não gostasse daquilo que escrevia, reescreveria o artigo. O ezine que era para ser simples cresceu com seções como FAQ, história, melhores artigos (IMHO) e uma seção de notícias que era tão difícil de manter que eu a converti num blog (http://barataeletrica.blogspot.com - postava tanto que o google me perguntou se eu interessava experimentar ter uma conta do recém inaugurado gmail). Se eu escrevesse qualquer coisa, haveria sempre uma referência, um link ou origem de onde tirei a informação. Não fui eu que disse, vão processar outra pessoa.

As pessoas começaram a oferecer serviços tipo: como melhorar meu html (muuuito pobre) e acesso a web sites. De graça. Eu recusei. Comecei sozinho, ninguém queria perder seu tempo me ajudando. Agora que eu era famoso, quem se importa? Além disso, um ezine melhor ficaria muito mais complexo. Meu foco não era de fazer melhores artigos para uma massa crescente de gente que estava conseguindo acesso a Internet. Do jeito que estava, já eram 3 a 4 emails por dia sobre "quero ser hacker, me ensina".

Poderia e talvez deveria ter transformado isso numa empresa (quem sabe, eu poderia conseguir escapar do estouro da "bolha" da Internet). Mas aí eu teria que cobrar. Para falar a verdade, quando eu comecei nem o conceito de freeware era muito bem compreendido. Para mim, isso significava não ter que me preocupar em pagar salários, taxas, contabilidade, direitos do consumidor, aquela coisa toda.

Teria que registrar tudo tudo tudo. E aí, seria um alvo. Se alguém me processasse e eu perdesse, pronto: acabou. E os artigos que eu colocava quase sempre estavam no limite da legalidade. Não usava codinome, usava meu próprio nome.

Minha opinião era bastante respeitada. O suficiente. Entre outras coisas, posso dizer que ajudei a começar o papo sobre Linux no Brasil (obs: a imprensa escrita, quando falava de informática, não mencionava o S.O., até aparecer um artigo no fanzine). Phiber Optik veio no Brasil (eu não tinha grana nem me convidaram para a palestra dele) mas eu dei dica para todo mundo perguntar para o cara, fazer uma comparação entre a segurança do Windows vs. a do Free BSD (repórters daquele período não sabiam nada disso – gerentes de informática também não). E perguntaram.

Eu também estava lá para dar suporte técnico quando a ativista da Anistia Internacional, Fernanda Serpa começou o movimento "Support Kevin Mitnick", que correu paralelo ao Free Kevin (não foi do movimento Free Kevin a idéia de demonstrar que o Mitnick estava preso sem julgamento há tempos, coisa impensável numa democracia, sem essa idéia ele poderia estar ainda lá). Antes dela começar eu já repetia que o sujeito não podia ser culpado de tudo aquilo, tinha coisa errada. Quando houve um blá-blá-blá de trazer Markoff e Shimamura numa conferência de US$ 400 por cabeça, muita gente queria ouvir os autores do "O Pirata e o Samurai", best-seller. Eu escrevi um artigo no ezine e depois de um tempo, nunca mais ouvi falar de alguém querer trazer esses caras aqui no Brasil. Se vieram, foi como turistas.

Minha tarefa estava completa. A "cena hacker" tinha acontecido. Não era mais um sonho. Haviam encontros de ratos de computador, 2600 e gente falando sobre isso em tudo quanto é lugar. As pessoas sabiam a diferença entre "hackers do bem" e lamers. Mas a imprensa continuou a publicar artigos ensinando coisas ruins só pelo prazer da coisa. Um número da extinta edição brasileira da Internet World me surpreendeu. Quase tudo era sobre coisas ruins de hackers. Havia material que podia ser usado para se aprender a "nukar" PCs rodando Win 95. Minha sorte: eu neguei uma entrevista. Talvez me considessem parte de um grupo maléfico. Outras revistas fizeram artigos semelhantes (praticamente resumiam livros). E alguns caras começaram a escrever livros usando material dos ezines. E eram um sucesso, mesmo que o que estivesse nos livros não funcionasse mais. Fácil provar que o vandalismo eletrônico do Brasil de hoje vem desses livros e revistas.

O congresso "hacker" que eu planejava nunca aconteceu (várias razões). A Internet comercial estava se espalhando rápido e eu não tinha um diploma de Ciência da Computação (2). Meu conhecimento era baseado em Unix e ficou desvalorizado numa primeira etapa, todo mundo, as empresas em geral adotaram Windows para tudo o que era relacionado na Internet. Como a maioria dos "dinossauros", não acreditava numa Internet comercial, dancei. E ao invés de montar empresa (o pessoal do Cadê, do Yahoo com certeza não sabia muito mais do que eu), fui fazer pós. Minha idéia era usar minha signature e lema "I login, therefore I am" (podem checar no google ou na Usenet, sou o autor dessa sentença), transformar essa idéia num trabalho acadêmico que poderia também conter minhas experiências começando a cena "hacker" brasileira.

As pessoas ficavam me pressionando direto por um livro sobre todos os meus sucessos, não uma tese. O fato é que coletei dados o suficiente para escrever um tanto sobre aqueles dias. Só alguns números do fanzine já fornecem material para 2 ou 3 livros. Algum dia vou fazer isso. Hoje, escrever um livro apenas para ganhar dinheiro seria me vender. E dinheiro, eu poderia ter feito isso até mesmo com um cartão "sou amigo do autor do fanzine Barata Elétrica". Um ex-amigo meu teve sua divída de R$ 40 perdoada, só porquê me apresentou ao devedor. Desse jeito.

Se quisesse escrever sobre "como fazer hacking", teria feito muito antes e ganhado, fazendo palestras (um "esperto" chegou a me tentar com isso, no início da minha fama). As pessoas algumas vezes me descrevem como um paranóico. Aliás "O Paranóico", na ausência de uma palavra melhor (música para trilha sonora: "Veteran of psychic wars" Blue Oyster Cult). Sempre.

De fato, tão logo eu descobri que algumas pessoas estavam querendo ficar do meu lado por conta do "hacking dark side", a nóia aumentou.

Com jornalistas e gente da imprensa também. Quando me arrumaram um contato (supostamente) da Suellete Dreyfus (autora do livro e tese "Underground", sobre a cena "hacker" na Austrália), supostamente ela estava querendo me entrevistar, declinei a oferta.

Algumas vezes até mesmo perdi "amigos" porque eles desistiram que eu escrevesse sobre eles. Então mudei algumas coisas. Sempre avisava que meu foco era em ética hacker e busca de conhecimento. Mudei meu jeito de escrever para evitar os cntrl-c-cntrl-v. Ainda é sobre "hacking" mas dentro de um ponto de vista mais amplo. Como se ensinaria sobre "hacking" sem usar computadores? Pode-se perfeitamente aprender sobre "hacking" sem "brincar com computadores". Alguns leitores disseram que continuariam lendo. E eu mantive o ezine e o blog por ser um desperdício parar com os dois.

Algumas vezes, vale a pena fazer um blog. Uma vez postei que precisava de uns chips de memória para meu computador 486 (usava como máquina de escrever). Um cara do Rio de Janeiro, Marcos Pereira, especialista em Free BSD, leu meu blog, pediu meu endereço postal e mandou os chips. Junto com outras coisas, num total de 16 kg de hardware, uma CPU completa feita de peças que ele catou com os amigos. Fizeram uma festa, as pessoas trouxeram coisas, ele montou um Pentium 233, 30 gig HD, via SEDEX. O micro ainda funciona até hoje (um amigo ficou babando de inveja quando viu a qualidade da placa da CPU). Que que a gente faz com um cara desses? Mandei umas camisetas do fanzine agradecendo.

Aí uns anos atrás, ele fez isso de novo, dessa vez um Pentium 4, 150 gig HD. Com monitor. E algumas revistas de ficção científica com reportagens sobre Asimov, Wells e Júlio Verne. Minhas leituras favoritas do tempo de infância e adolescência. Talvez esse cara seja um dos 35 homens justos, cuja existência impede Deus de destruir a terra. Não sei.

O problema, quando se escreve um ezine hacker hoje, é que tudo está facilmente disponível, todo mundo tem bem mais acesso do que no tempo em que comecei. E há muita gente que alega ter conhecimentos "hacker". Mesmo o Youtube tem vídeos sobre inseguran-ça computacional. Não se precisa ir no "underground" para se aprender sobre "assuntos subversivos". Minha opinião, é preciso se ter consciência, bom senso, o assunto principal no fundo das matérias, desde o primeiro número. Se você escreve sobre como fazer isso, isso fica velho rapidinho. Quando você escreve sobre como pensar acerca disso, a coisa continua útil sempre. Quem quiser pode pegar velhos números do fanzine e ainda achar bom material, capaz de salvar sua pele algum dia.

Muito ruim que eu não escrevi uma tese sobre meus feitos. Não sou tão conhecido fora do Brasil, apesar dos meus artigos na 2600-Hacker Quaterly. O fato de que eu não escrevi um livro também pega. Como poderia escrever um livro sobre "iniciar uma cena hacker" e ainda conseguir um emprego "normal" em qualquer lugar mas em segurança informática? Já houve várias conferências "hacker" em São Paulo. Inclusive moro na cidade. Mas houve vezes em que não podia ir. Muitas câmeras de TV.
Exemplo: numa conferência específica, eu estava trabalhando próximo a uma sala onde estava um pessoal encarregado de processar o Youtube. Puxa, até a legislação que estava sendo consultada eu via na minha frente. Esse pessoal tinha que saber do meu passado? Deveriam saber? Já em outra, pude ir, me garantiram menos câmeras e nenhuma da TV.

Também tem o fato de que as pessoas sempre cobram mais se sabem que você é famoso. Durante muito tempo estudei esses casos de celebridades instantâneas e coisas a respeito de como lidar com fama. No futuro, todo mundo vai ter que lidar com isso (para ser mais exato, alguém colocou um link de um texto meu (http://migre.me/1unAF) sobre isso no orkut sobre a Geisa da Uniban, bem no início daquela história, só que não dá para dizer até que ponto isso influenciou).

A maioria das pessoas conectando com a Internet não sabem nada disso e perdem ótimas oportunidades. Aconteceu, antes da pessoa se acostumar com isso, já foi. As pessoas tem que se conscientizar que ficar famoso não é um conto de fadas. Para se fazer bom uso disso, tem que se saber a respeito. Você publica alguma coisa no Youtube ou num blog, será lembrada pela eternidade. Você cresce, muda, envelhece. Mas seu passado continua lá. Do jeito que foi. Minha grande sorte foi que eu escrevi coisas pensando. Não tenho muito remorso sobre isso.

Quando se é famoso, algumas pessoas acabam conhecendo você porquê eles estão ficando famosos na mesma época mas com outras ocupações. Como o delegado de polícia Mauro Marcelo, primeiro "cybercop" brasileiro. Chegou a responder email meu com um pedido de entrevista (que acabou não acontecendo). Na época ele estava como chefe da ABIN, me conhecia (quase todo mundo me conhecia de ouvir falar, por volta de 1995, 96) e isso poderia ter facilitado um acesso. Claro que ele nunca me "pegaria" ou me "prenderia". Parei com qualquer coisa parecida com ilegalidade quando comecei o fanzine.

Talvez ainda faça alguma coisa mas nem preciso fazer. Hoje em dia, o acesso é muito mais fácil. A palavra mágica "por favor" funciona bem. Se a pessoa não me conhece, me apresento. Procuro gente que me conhece.

Estava sem dinheiro nenhum para ir na Campus Party e queria ver o Kevin Mitnick de perto. O pessoal da organização nunca tinha ouvido falar de mim (Trilha sonora: Fame - Irene Caras...). Mas consegui entrar lá com convite e tudo (a little help from my friends - Beatles). E com um pouco de jeitinho, praticamente furei a fila de credenciamento, cheguei no final mas ainda consegui chamar a atenção dele, já estava indo embora (parecia cena de guerra, faltou o gás lacrimogênio e helicóptero baixando), mas catei o cartão dele com o email e fiz contato.

Aí foi que nem na música.. "Let me please introduce myself.." (Speak of the devil - Rolling Stones). Mesmo ele sendo bastante legal com os fãs (muita gente se fotografou ao lado dele e fez até vídeos para colocar no orkut), podia acontecer de não conseguir um encontro.. Acho que o fato de que eu falo um inglês fluente, conheço outras personalidades da Internet, experiência internacional, o envio deste artigo publicado na 2600 – Hacker Quaterly, tudo isso ajudou um pouco. Consegui marcar um encontro, jantamos num lugar e ainda fomos numa casa noturna, até as 4 da manhã. O cara é legal, não tem um pingo de arrogância.

Agora são 16 anos do Fanzine Barata Elétrica (saindo quase bi-anual). Uma grande experiência. Boa parte dela é culpa dos leitores. Dá uma sensação muito legal quando se encontra alguém cuja vida mudou por causa de um artigo escrito por você. Não fiquei rico (pelo contrário, ainda corro muito atrás de dinheiro), mas aprendi bastante. Desde legislação, direito autoral, editoração, marketing, rh, até mesmo jornalismo. Falta só aparecer em algumas conferências pelo mundo afora (depende delas acharem minha história interessante ou não) e lançar um livro contando as experiências. "Don't you.. forget about me" (Simple Minds)..

Isso pode acontecer com você também.

Acredito que todo mundo deveria escrever o seu próprio fanzine, blog ou mesmo twitter. Alguém já disse alguma vez em algum lugar: se você não gosta das notícias, sai e vá fazer algumas. Todo mundo pode ajudar a melhorar o mundo, com pequenas coisas. Simplesmente ajude sua comunidade.

Comecei com algo enviado para umas poucas pessoas que usavam a rede num laboratório de informática. E cheguei onde estou. Pense a respeito.

Boa sorte.

(*) O que eu aprendi sobre direito autoral, legislação e etc mais do que o suficiente para entender que não valia muito a pena. Apesar que posso mudar de idéia.

(1) Já encontrei pessoalmente um ou outro membro do AXUR 05. No início eles me xingavam muito. Nos últimos números, ficaram mais amigos.

(2) Sou formado em Letras-Alemão e terminando 2a graduação em Ciência da Informação.

Derneval Ribeiro Rodrigues da Cunha

Criador do primeiro fanzine (revista de fã) Barata Elétrica, dedicado a segurança informática.

Auto-didata, Usa computadores e interage com "ratos de computador" desde 1983, tendo começado na Internet em 1993.

Publicou diversos textos em revistas como Internet World, 2600-Hacker Quaterly e Datenschleuder.

Formação e qualificações: Curso de PHP, SQL e JAVA pela Seprosp-SP (2010), Letras-Alemão (USP), Ciência da Informação (USP), Mestre pelo Programa de Pós-Graduação em Integração da América Latina da Universidade de São Paulo (PROLAM/USP).

Você quer a sua empresa em contato com os melhores profissionais de Segurança da Informação???

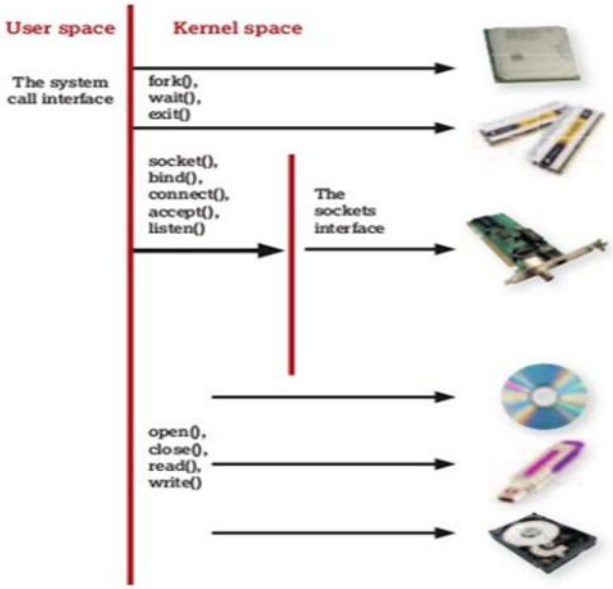
Então a sua logomarca deveria estar aqui.

contato@staysafepodcast.com.br

Ao procurar a definição da palavra "Kernel" em um dicionário (inglês/inglês) percebi que ele deu ênfase ao seguinte ponto: “The most important part of a statement, idea, plan, etc” e também “a very small part or amount of something”. A partir daqui já temos uma idéia de que é algo muito importante, pois mesmo sendo muito pequeno o kernel é o "cara" que gerencia a interface de comunicação entre o hardware o os programas instalados no computador. Quando falamos do Linux estamos falando exclusivamente deste kernel, todo o resto como gnome, firefox e até mesmo o bash tratam-se apenas de programas que rodam no Linux e não fazem parte do Sistema Operacional (kernel linux).

Entendendo o Kernel

OK, mas o que exatamente faz esse tal de kernel? A figura a seguir mostra de uma forma geral como o kernel disponibiliza serviço para os aplicativos rodando através de inúmeros pontos de entrada conhecidas como chamadas de sistema (system calls).



O kernel utiliza chamadas de sistema como leitura e escrita para prover acesso ao hardware.

Do ponto de vista de um programador isso parece uma função comum, embora na realidade uma chamada de sistema envolva diferentes interruptores no modo de operação do "kernel space" para o "user space" Juntos esse conjunto de chamadas de sistema formam uma especie de "maquina virtual" que trabalha antes do hardware real. Um exemplo claro disso é o sistema de arquivos.

Kernel Modular

Agora que entendemos melhor o que o kernel faz, vamos olhar mais atentamente a sua organização física. As primeiras versões do kernel eram monolíticas, ou seja, todos os módulos estavam compilados dentro de um único arquivo executavel. O kernel das distribuições mais novas são modulares, ou seja, os módulos podem ser carregados no kernel em tempo de execução, isso faz com que o núcleo do kernel fique menor e não seja necessário reiniciar a maquina para carregar ou substituir novos módulos.

O núcleo do kernel é carregado na memória na hora do boot e é lido de um arquivo no diretório "/boot" na maioria das vezes este arquivo é chamado de "vmlinuz-VERSÃO_DO_KERNEL".

Para ver a versão do kernel corrente utilize o comando:

```
---
#uname -r
---
```

Os módulos ficam no diretório "/lib/modules/VERSÃO_DO_KERNEL/"

Gerenciando módulos.

Veremos agora alguns comandos para gerenciar os módulos do seu kernel, como por exemplo o comando para listar os módulos carregados que é o "lsmod", o lsmod vai mostrar uma saída semelhante a esta:

```
---
Module                  Size  Used by
vfat                   14464  0
isofs                  36388  0
fat                    54556  1 vfat
nfs                   262540  0
lockd                  67720  1 nfs
nfs_acl                4608  1 nfs
sunrpc                 185500  5 nfs,lockd,nfs_acl
bridge                 55576  0
tun                    12672  0
usb_storage             73792  4
libusual               19236  1 usb_storage
---
```

Esta saída possui quatro campos divididos por nome do módulo que esta carregado, o tamanho do módulo, quantas vezes ele esta sendo utilizado e quais os módulos que dependem dele.

Podemos carregar um módulo utilizando o comando "modprobe" (podemos também utilizar o comando "insmod" porém o modprobe é mais aconselhavel pois ele resolve as dependências do módulo).

Outro ponto muito importante na saída do comando lsmod é o terceiro campo que indica a quantidade de vezes que o módulo esta sendo utilizado pois o linux não vai permitir a remoção de um módulo cujo o campo used seja diferente de zero, no exemplo acima vemos o módulo "isofs" (utilizado para dar suporte ao sistema de arquivos "ISO" que é utilizado em CDs) com o campo used "0" neste caso podemos remover o módulo com o comando "modprobe -r isofs", após executar este comando o módulo isofs não vai aparecer mais quando executarmos o lsmod.

Não é muito comum carregar módulos manualmente no dia a dia, porém se você precisar carregar um módulo manualmente poderá incluir parâmetros específicos de cada módulo, como no exemplo a seguir:

```
---
modprobe usb_storage delay_use:3
---
```

No exemplo supra-citado habilitamos o parâmetro "delay_use:3" para o módulo "usb_storage" que define um time-out de 3 segundos para o módulo procurar um novo device. Para saber quais as opções de cada módulo utilizamos o comando modinfo como no exemplo a seguir:

```
---
# modinfo usb_storage
filename:       /lib/modules/2.6.24-23-generic/kernel/drivers/usb/storage/usb-storage.ko
license:        GPL
description:    USB Mass Storage driver for Linux
author:         Matthew Dharm <mdharm-usb@one-eyed-alien.net>
srcversion:     99E0EB653929DE200DF6AF9
depends:        libusual,usbcore,scsi_mod
vermagic:       2.6.24-23-generic SMP mod_unload 586
parm:           delay_use:seconds to delay before using a new device (uint)
---
```

A linha que nos interessa neste caso é a que começa com "param" que mostra os parâmetros aceitos pelo módulo. Caso você possua a source do kernel você também pode encontrar uma documentação muito útil em "/usr/src/VERSÂO_DO_KERNEL/Documentation/kernel--parameters.txt"

Sistema de arquivos /proc

O kernel também nos fornece inúmeras informações que podem ser encontradas no sistema de arquivos "/proc", os arquivos no /proc são criados pelo kernel (alguns você pode alterar, outros não) um exemplo claro do tipo de informação que podemos encontrar no /proc está no arquivo "/proc/modules" que mostra todos os módulos carregados no sistema (sim é semelhante ao comando lsmod.. =D), no arquivo "/proc/meminfo" que mostra o status detalhado da memória do sistema e também o arquivo "/proc/net/arp" que mostra a tabela ARP (mesma tabela exibida pelo comando "arp -a").

Beleza falei do /proc mas só citei arquivos que não podem ser alterados, são arquivos que somente nos fornecem algumas informações, mas o /proc não é só isso, um subdiretório do /proc muito importante é o "sys", por exemplo o arquivo "/proc/sys/net/ipv4/ip_forward" define que o kernel irá encaminhar pacotes IP, a sintaxe é muito simples se o conteúdo deste arquivo for "0" (zero) o kernel não fará encaminhamento de pacotes IP e se o conteúdo for "1" (Um) o kernel fará encaminhamento de pacotes IP, esta opção deve ser habilitada se você for utilizar o linux como um roteador; Tá, mas como eu habilito isso?

Vamos primeiro ver como esta o arquivo:

```
---
# cat   /proc/sys/net/ipv4/ip_forward
0
---
```

Vemos que o conteúdo do arquivo é “0” (zero), agora vamos habilitar o encaminhamento de pacotes IP no kernel.

---

echo 1 > proc/sys/net/ipv4/ip_forward

Pronto agora o encaminhamento de pacotes IP esta habilitado, fácil né? Porém tem um pequeno problema aqui, se reiniciarmos a maquina este arquivo voltara a ter conteúdo igual a “0” (zero). E como solucionamos isso? A solução é muito fácil. Utilizamos o arquivo “/etc/sysctl.conf” para definir os valores que serão configurados na hora do boot, então basta acrescentarmos a linha “net.ipv4.ip_forward = 1” no arquivo sysctl.conf.

Melhorando a performance.

Muitos dos parâmetros do /proc/sys que permitem escrita podem ser utilizados para melhorar a performance do Linux. Um exemplo de como podemos modificar o kernel para melhorar a performance de acordo com o tipo de aplicação que você vai utilizar está no guia de instalação do Oracle 10g que pede pra você configurar alguns parâmetros como o “kernel.shmmax=2147483648” definindo o tamanho máximo de segmento de memória partilhada para 2GB.

Outra modificação que podemos fazer é definir que nossa máquina não vai responder por broadcast de icmp (o bom e velho ping -b 255.255.255.255) configurando o sysctl da seguinte forma:

---

sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1

Agora fica a seguinte dúvida, pra ver os valores eu vou ter que dar cat de arquivo em arquivo ou saber todos os caminhos do comando sysctl? Claro que não, basta utilizar o comando sysctl -a que ele vai exibir todos os parâmetros e seu valores, porém, ele não mostra para que serve cada um deles para isso podemos encontrar os detalhes no bom e velho “man proc”.

Ta vendo, o kernel não é aquele bicho de sete cabeças que muitos imaginam....rsrsr

Cleber Brandão (CleBeer)

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.

H2HC

www.h2hc.com.br

HACKERS TO HACKERS CONFERENCE SEVENTH EDITION

Brasil - São Paulo

25 a 30 de Novembro de 2010

Hotel Novotel Morumbi

Palestrantes Confirmados*

Anchises de Paula
Bruno Oliveira
Carlos Sarraute
Eric Filiol
Filipe Balestra
Jeremy Brown
Matthieu Suiche
Nelson Brito
Ranieri Romera
Rodrigo Branco
Rodrigo Montoro
Sergey Bratus
Wagner Elias

*Lista final será apresentada após o fechamento do call for papers.

Treinamentos

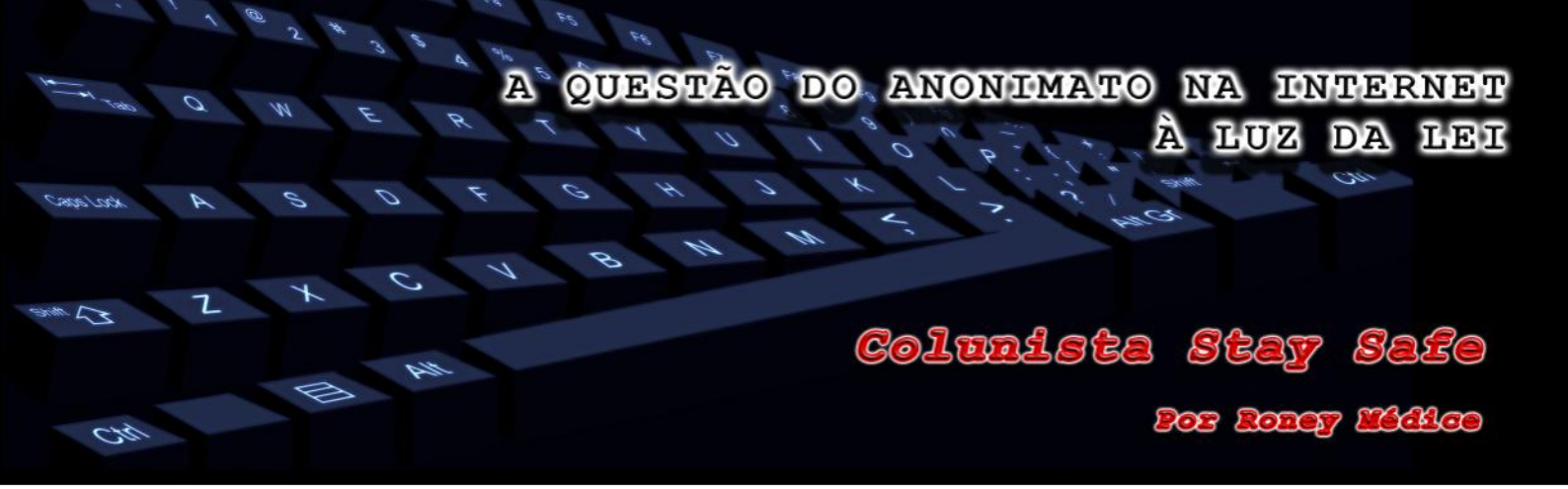
1- Web Testing & Exploiting Workshop
Instrutor: Nahuel Grisolia

2 - Windows physical memory acquisition and analysis
Instrutor: Matthieu Suiche

3 - Advanced Disk Forensics
Instrutor: Tony Rodrigues

Patrocínio

Check Point SOFTWARE TECHNOLOGIES LTD. | Microsoft | SecureWorks | symantec. | nitrosecurity
TENABLE Network Security* | iDEFENSE | CONVISO IT SECURITY | BRCONNECTION | TREND MICRO
RMF SECURITY | Trustwave Security begins with Trust | IMMUNITY | SOURCEfire | CORE SECURITY TECHNOLOGIES



A QUESTÃO DO ANONIMATO NA INTERNET À LUZ DA LEI

Colunista Stay Safe

Por Roney Médice

Com o advento da criação da Internet, a partir da década de 90, muitas pessoas puderam trabalhar em conjunto, compartilhando dados, informações e documentos nessa grande rede de computadores. Ocorreu uma expansão explosiva da Internet nessa época, motivada por falta de uma administração central assim como à natureza aberta dos protocolos da internet. O acesso a um grande número de informações disponíveis às pessoas, com ideias e culturas diferentes, pode acarretar tanto em uma melhora dos conceitos da sociedade como um declínio, dependendo das informações existentes na internet e por quem as disponibilizam.

Em tempo de internet onde existe uma grande mobilidade tecnológica, percebemos que a cada passo dado em nossa "vida digital", deixamos rastros de informações e dados confidenciais pela grande rede de computadores. Novidade? Até que não, pois somos "antenados" na tecnologia e queremos ter status, procuramos nos divulgar da melhor maneira possível fazendo o que conhecemos como Marketing Digital.

Entretanto, em alguns momentos durante a nossa navegação na grande rede de computadores (Internet), temos a oportunidade de comentar alguns artigos publicados na internet, com o qual podemos concordar ou discordar do caminho traçado pelo autor.

Em muitos casos e acredito que seja a maioria, quem gosta de opinar sobre um determinado conteúdo publicado no site ou blog, deixa registrado o nome e sobrenome assim como o e-mail de contato para um possível contato no futuro.

Esse procedimento deveria ser seguidos por todos, no qual você se identifica e opina sobre um determinado assunto, gerando uma expectativa ao autor do artigo que ficará muito feliz em saber que pessoas se interessaram pelo seu conteúdo e estão dispostas a trocar ideias. Nada mais frustante é alguém ler o seu material publicado e no final, não se identificar para fazer o comentário, escrevendo vários absurdos atacando o próprio autor, ocorrendo em crimes de Calúnia, Difamação e Injúria, estes tipificados em nosso Código Penal Brasileiro nos Artigos 138, 139 e 140, respectivamente.

Todavia, temos que ter a consciência que em nossa Carta Magna, a Constituição Federal Brasileira de 1988, entre os seus dispositivos mais importantes, destaco um que trata dos direitos e deveres individuais e coletivos, descrito no artigo 5º inciso IV que preceitua "IV – é livre a manifestação do pensamento, sendo vedado o anonimato". Ou seja, todo cidadão tem o o direito de expressar o seu pensamento, manifestar o seu ideal publicamente porém, não pode ser de forma anônima pois é vedado (proibido) pela nossa Constituição Federal.

Analisando o texto desse inciso, podemos realmente notar qual era a preocupação do legislador da época em que a Carta Magna foi promulgada. Imagine se os meios de comunicação, que na época se resumiam aos jornais impressos, televisão e rádio, começassem a divulgar informações inverídicas sobre determinadas pessoas, empresas, políticos e etc, de tal forma a criar constrangimentos, prejuízos à imagem das empresas e outras consequências em que a vítima não possa identificar o autor desses fatos. Seria um desastre nas relações pessoais e para a própria economia, pois sem a identificação do autor do manifesto, não haveria a possibilidade da vítima se defender ao ponto de cessar as provocações e além disso, como poderia alguém ser responsabilizado pelos danos causados?

Nos dias atuais, se existem processos no judiciário com lides sobre os crimes de calúnia, difamação e injúria, é porque existe um autor identificado para responder pelos os seus atos. Mesmo que o autor seja o provável, sem a devida comprovação, pois isso será discutido no mérito da lide. Mas teremos sempre um "suspeito", com base na vedação do anonimato.

Diversos sites de conteúdo já se preocupam com essa máxima do anonimato e nos seus controles de comentários aos artigos publicados, possuem configuração que determina que para ser adicionado um comentário, a pessoa tem que informar o nome e o e-mail de contato, evitando assim que o anonimato aconteça.

Todavia, sabemos que não é tão simples assim evitar o anonimato pois mesmo que seja necessário informar o nome e o e-mail para comentar um texto, o internauta pode simplesmente inventar um nome e digitar um e-mail inválido, pois não há checagem por parte do site a validação dos dados informados. Estará esse comentário em situação "ilegal" perante a Lei?

É uma questão que rende muita discussão em torno do assunto pois no momento que se informa qualquer nome adverso da identidade pessoal do comentarista, está atendido o preceito legal, pois não incorre no anonimato, porém, incorre em outra situação que, nesse caso, caracteriza um crime tipificado no Código Penal Brasileiro, o de Falsidade Ideológica conforme o Artigo 299.

Um exemplo de um caso que envolveu a questão do anonimato na internet e muito difundido na mídia, foi o caso do Google que teve que indenizar um cidadão que foi alvo de ofensas realizadas no site de blog da empresa. O juiz do processo determinou que o Google retirasse oito páginas do blog com conteúdos ofensivos ao autor da ação sob pena de uma determinada multa diária.

A sentença, ao final do processo, foi proferida e o Google foi obrigado a pagar uma quantia a título de indenização moral. A empresa recorreu alegando que ela não poderia ser responsabilizada pelo conteúdo criado por seus usuários mas a desembargadora do caso confirmou a sentença esclarecendo em seu despacho que "à medida que a provedora de conteúdo disponibiliza na internet um serviço sem dispositivos de segurança e controles mínimos e, ainda, permite a publicação de material de conteúdo livre, sem sequer identificar o usuário, deve responsabilizar-se pelo risco oriundo de seu empreendimento".

A proibição ao anonimato é ampla, abrangendo todos os meios de comunicação, mesmo as mensagens de internet.

Não pode haver mensagens injuriosas, difamatórias ou caluniosas. A Constituição Federal veda o anonimato para evitar manifestações de opiniões fúteis, infundadas, inverídicas que tem como propósito: intuito de desrespeito à vida privada, à intimidade, à honra de outrem conforme o caso acima citado.

Recentemente, o Marco Civil da Internet recebeu diversas sugestões para melhoria nas regras e normas de utilização da internet. Dentre elas, uma questão levantada é sobre o anonimato na internet, uma situação essa bem peculiar e caracterizado pela "vida moderna" que temos. No meio digital, não é difícil utilizar ferramentas e artifícios para navegar "anonimamente" como o sistema Thor e outras soluções que aumentam ainda mais a capacidade de navegação sem ser descoberto a sua própria identidade.

Claro que vestígios de acesso vão ocorrer como a identificação do IP que será registrado no momento de comentar um artigo, o log do provedor de internet para identificar o autor do acesso vinculado ao IP rastreado e outras ações que poderão levar ao verdadeiro responsável pela manifestação do pensamento, registrado no blog.

Entretanto, conforme já comentado em outros artigos, essa identificação pode ser totalmente sem sentido quando nos deparamos com várias redes sem fio (wireless) desprovidos de nenhum tipo de criptografia de conexão, fazendo assim, com que qualquer pessoa possa utilizar essa rede para registrar um comentário ofensivo sem ter realmente a sua identidade revelada.

Contudo, o anonimato na internet é legalmente vedado porém esse assunto é palco para muita conversa e discussão que precisamos nos unir para chegar em um determinado nível de aceitação pela sociedade. Mesmo que a Lei vede o anonimado, hoje é o que mais vemos acontecer nas mídias sociais com a criação de perfil fake (falso), apelidos como se fossem nomes verdadeiros e outras situações que só trazem problemas para as vítimas desses baderneiros digitais.

Roney Médice

Coordenador de Segurança da Informação do Terminal Retroportuário Hiper Export S/A;

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 ES;

Graduado em Ciência da Computação e Direito;

MBA em Gestão de Segurança da Informação e

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