Álvaro Vilobaldo Rios da Silva (711605-1)
Douglas Botelho (71170847)
Marcio Fernandes Justino (7116006-1)

Workshop Cibercrime

São Paulo – SP

13 de novembro de 2012

Álvaro Vilobaldo Rios da Silva (711605-1)
Douglas Botelho (71170847)
Marcio Fernandes Justino (7116006-1)

Workshop Cibercrime

Workshop de Cibercrime com foco em fraudes desenvolvido para a disciplina do 2º Semestre de Fraudes Corporativas do Curso de Pós-Graduação em Computação Forense

Professor Antônio Carlos Gesteira

PÓS-GRADUAÇÃO LATO SENSU EM COMPUTAÇÃO FORENSE
UNIVERSIDADE PRESBITERIANA MACKENZIE DE SÃO PAULO

São Paulo – SP

13 de novembro de 2012

Sumário

Eles já provaram que são sem escrúpulos.
E se, um dia, uma rede terrorista resolver empregá-los?
(Igor Lopes - Jornalista)

Introdução

Esse documento é fruto dos estudos elaborados para o trabalho da disciplina do 2º Semestre de Fraudes Corporativas ministrado por Antônio Carlos Gesteira do Curso de Pós-Graduação Lato Sensu em Computação Forense da Universidade Presbiteriana Mackenzie de São Paulo.

O que é cybercrime? Como combatê-lo? Como evitá-lo? Isso é possível? Essas foram algumas das perguntas que nos fizemos durante o desenvolvimento desse trabalho e que condensamos nesse workshop vamos falar sobre os principais crimes praticados pelos meios eletrônicos, contudo sendo um tema demasiado complexo e abrangente apresentando constantemente novas tecnologias e novas formas de operação do crime não será possível mostrar tudo a respeito do mesmo.

Objetivo

Este workshop tem por objetivo ampliar os conhecimentos sobre Cybercrime, dissertando sobre as fraudes praticadas, alguns casos reais, o modus operandi do criminoso, as prevenções, o processo de forense em Cybercrime e a forma de combate ao Cybercrime sempre embasando em fontes confiáveis para os dados apresentados. O workshop deve ser concluído até o dia 20 de Junho de 2012, quando será entregue em meio digital, impresso e apresentado pelos seus integrantes.

1 Cibercrime

> For hard cash, we will lie and deceive
> Even our masters don't know the web we weave
>
> Dogs Of War - Pink Floyd

Segundo o livro *Desvendando a Computação Forense* (MACHADO; ELEUTÉRIO, 2011), existem dois tipos de crimes ligados aos computadores. No primeiro, o computador é uma ferramenta para a prática do ilícito, como seria o papel ou caneta; já o outro o computador é próprio meio do crime, ou seja, sem o mesmo o crime não poderia acontecer.

De acordo com *Incident Response: Computer Forensics Toolkit* (SCHWEITZER, 2003) o *Departamento de de Justiça* norte americano prevê três ocasiões onde o crime se comuta com a computação, sendo eles, quando o computador é o alvo de ataque (virus, malware, invasão, phishing), serve para armazenamento de dados crimosos (contabilidade de traficantes) e como ferramenta para cometer o delito (plano do crime num documento).

Como vimos, o departamento de justiça norte americano ainda define mais uma forma do computador estar envolvido em atos ilícitos a qual seria o armazenamento de dados crimosos como é o caso da contabilidade contida num arquivo do Excel[1] referente ao tráfico de drogas. Contudo ao armazenar informações no computador o mesmo estaria sendo usado como ferramenta.

Já a Wikipédia (WIKIPÉDIA, 2012) define cybercrime da seguinte forma:

> Crime informático, e-crime, cybercrime, crimes eletrônicos ou crime digital são termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores é utilizada como uma ferramenta, uma base de ataque ou como meio de crime.

O que podemos afirmar com base nas referências e lógicas mostradas acima é que cibercrime é todo crime que tem o computador ou redes como seu principal meio.

[1] Microsoft Excel

1.1 Crimes de informática mais comuns

"Segundo o IPDI (Instituto de Peritos em Tecnologias Digitais e Telecomunicações), pessoas que usam a informática para roubar identidades podem responder por estelionato, furto mediante fraude, intercepção de dados, quebra de sigilo bancário e formação de quadrilha." (CARPANEZ, 2012)

- Roubo de Identidade: os internautas são enganados tendo sua identidade tomada para realização de compras on-line, transferências financeiras indevidas, etc;
- Pedofilia: criação de sites e/ou fornecimento/compartilhamento de material relacionado ao abuso sexual infantil;
- Calúnia e Difamação: divulgação de informações não verídicas, prejudiciais à vítima. Muito comum nos sites de relacionamentos;
- Ameaça: e-mail, post em sites, com intuito ameaçador à vítima;
- Discriminação: divulgação de conteúdo relacionado ao preconceito - raça, religião, cor, etnia, procedência. Também muito comum com o crescimento das redes sociais;
- Fraudes; e
- Espionagem Industrial: aquisição de informação sigilosa de uma empresa por um concorrente. Com o avanço tecnológico e a falta ou falha de controles de segurança, essa prática tem se intensivado, sendo facilitada pela quantidade de informações que se pode carregar em um dispositivo móvel.

1.2 Fraudes

Como pode ser observado nos estudos da CERT.br (CERT.BR, 2012) apresentado na figura 1.1, a fraude é um dos incidentes com maior ocorrência na atualidade.

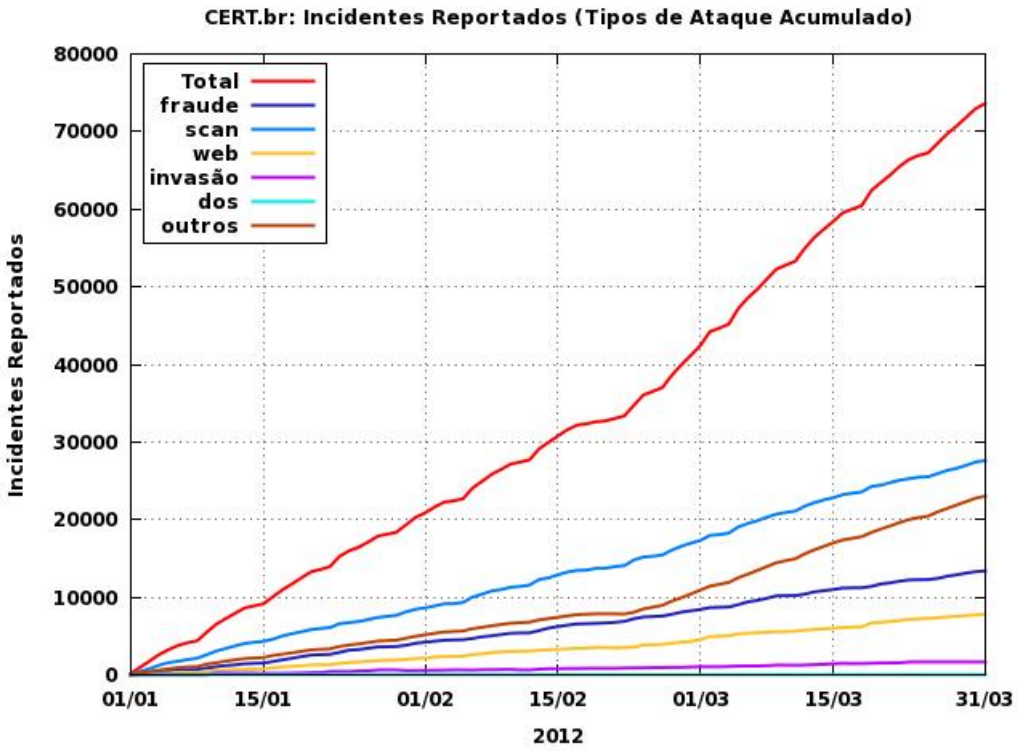

Figura 1.1: Incidentes Reportados - 2012

Dentro dos incidentes de fraude reportados pela (CERT.BR, 2012), pode-se constatar que a utilização de páginas falsas para ludibriar o usuário ocupa a maior faixa de ocorrências, atingindo mais de 50% dos incidentes, o que pode ser demonstrado na figura 1.2.

Figura 1.2: Tentativas de Fraudes Reportadas - 2012

1.2.1 Agentes da Fraude

Os agentes de fraudes podem ser de origem externa (o invasor sem confiança) ou interna (funcionários com total confiança pelos sistemas da corporação). Algumas fraudes mais elaboradas apresentam a participação de ambos agentes, sendo esta uma das formas mais utilizadas por organizações criminosas.

Dentro das fraudes cometidas por agentes internos, quando em cargos de chefia, pode-se destacar o prejuízo acentuado causado à organização tendo visto em muitas vezes a falta de punição. (GIL, 1991, p. 18-20).

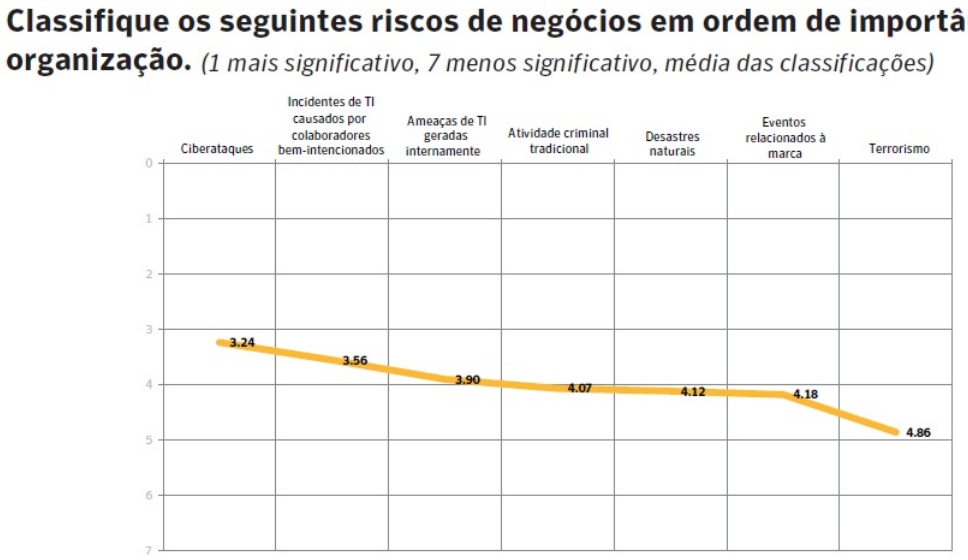

Figura 1.3: Riscos de negócios em ordem de importância para a organização(SYMANTEC, 2011)

Como mostra o relatório de segurança da Symantec[2], os incidentes de segurança causados por cibercrime e por agentes internos são considerados os de maior risco para as organizações. Assim como as ameaças mais significantes estão por conta da ação dos hackers, ou agentes externos.

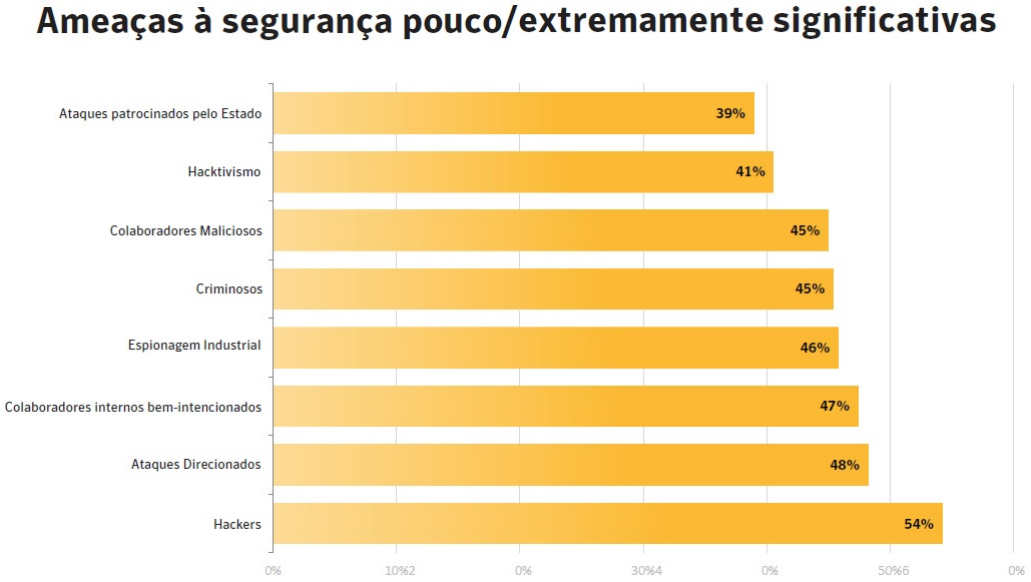

Figura 1.4: Ameaças à segurança pouco/extremamente significativas (SYMANTEC, 2011)

[2](SYMANTEC, 2011)

1.3 Cibercrime Brasileiro

O e-crime está cada vez mais envolvido com o crime convencional, “geralmente alimenta outros crimes, como o narcotráfico”, ressalta Fábio Assonlini, analista de malware da Kaspersky no Brasil.

O Brasil lidera o ranking com maior número de bankers do mundo. No Brasil o cibercrimosos envolvidos com o roubo de dados bancários e clone de cartões ficou conhecido como “Raul” (ADRENALINE, 2011). Os crimosos se vangloriam e expõem suas conquistas na própria internet, onde temos diversos exemplos de músicas que até mostram do modus operandi da coleta dos dados até a melhor forma de utilização (CARTãO, 2012). Os brasileiros foram os primeiros a criarem um banker rootkit para arquitetura x64 (64 bit).

1.3.1 Perfil do Banker Brasileiro

Em geral o perfil do banker brasileiro é jovem, de baixa renda, que obtém códigos maliciosos de outros (Figura 1.5) para aplicar seus golpes.

Figura 1.5: Anúncio de botnet (KASPERSKY, 2012)

Existem sites de comercialização de códigos maliciosos espalhados pela internet, e alguns inclusive com direito a reclamações de não entrega dos produtos (Figura 1.6).

Figura 1.6: ”Procon”do site de vendas (KASPERSKY, 2012)

Outro assunto pertinente e curioso a respeito do cibercrime brasileiros é que para começar na vida crimosa virtual com maior conforto e menos esforço existem até cursos onlines que ensinam atacar sites financeiros e a mandar spam (RODRIGUES, 2012b).

2 *Arquitetura Tecnológica*

Pela própria natureza do cibercrime ser diversa e abrangente, os equipamentos utilizados para a sua prática são tão diversos e amplos quanto. Mesmo que os computadores sejam o principal meio, nada impede que tablets, smartphones, roteadores etc sejam utilizados de alguma forma como meio para cometer o crime cibernético.

De forma análoga as tecnologias empregadas pelos equipamentos ou disponíveis para estes também são abrangentes. Segundo análises da Kaspersky Lab (KASPERSKY, 2012) é comum uma especialização de códigos maliciosos por região. Nos EUA o código malicioso mais comum são do tipo FAKEAV[1], na Europa oriental, Russia e países ibéricos são mais comuns rootkits, o Brasil entretando se especializou na produção de códigos maliciosos para furto de dados bancários e clones de cartão de créditos também conhecidos como bankers.

Como já foi dito o Brasil foi classificado como país líder em vírus que roubam dados bancários, também conhecido como trojans bankers, segundo pesquisa da Kaspersky Lab (RODRIGUES, 2012a), sendo o mesmo o 95% dos códigos maliciosos desenvolvidos no Brasil são justamente para esse intuito (ADRENALINE, 2010).

[1] Falsos antivirus

3 *Abordagem Metodológica*

Existem várias modalidades de criminosos digitais. A maioria dos ataques ($\cong 95\%$) é proveniente de pessoas com pouco conhecimento em atividades Hacker.

As mais comuns fraudes da atualidade são originárias de Phishing - tipo de fraude projetada para roubar informações valiosas particulares. O phishing, comumente chamado de phishing scam ou scam, utiliza-se de pretextos enganosos para obter de sua vítima informações relevantes tais como números de cartões de crédito, senhas, dados de contas, entre outros.

Para que o phishing funcione, o usuário mal-intencionado envia milhões de emails falsos que parecem vir de sites populares ou de sites nos quais se tem confiança, como site de uma instituição financeira ou de uma empresa de cartão de crédito. Esses emails, e os sites a que remetem, parecem oficiais o suficiente para convencer muitas pessoas de sua legitimidade. Acreditando que esses emails são legítimos, pessoas desavisadas com frequência respondem às solicitações de recadastros, número do cartão de crédito, senha, informações de conta ou outras informações pessoais.

Para fazer com que esses emails pareçam ainda mais reais, os criadores de scams podem colocar um link em um email falso que parece levar ao site legítimo, mas na verdade leva você ao site de scam ou mesmo a uma janela pop-up muito semelhante ao site oficial. Uma vez entrando em um desses sites, a vítima poderá, inadvertidamente, inserir informações pessoais, que serão transmitidas diretamente ao criador do site. Ele poderá usar esses dados para comprar bens, candidatar-se a um novo cartão de crédito ou roubar a identidade da vítima.

3.1 Caso Carolina Dieckmann

Um caso exemplar de phishing que ganhou a mídia nos últimos meses foi o caso da Carolina Dieckmann. No famigerado caso a atriz Carolina Dieckmann recebeu um spam solicitando o usuário e senha da sua conta de e-mail. Ao informar o dados a mesma concedeu acesso a sua conta do Gmail pelo qual a mesma havia enviados diversas fotos nuas e que ainda estavam

armazenadas nos *enviados*. Com as fotos em mãos os invasores chantagearam a atriz.

Veja a baixo um infográfico do caso.

Figura 3.1: Infográfico de um phishing scam

3.2 Modus Operandi

De maneira geral, o modus operandi é o comportamento necessário para a prática de um crime com sucesso. No mínimo, todo modos operandi deve envolver:

1. Assegurar o sucesso do crime;
2. Proteção da identidade; e
3. Fuga efeito.

Não se podem vincular casos pelo modus operandi, pois, o modus operandi é dinâmico, mudando com a experiência de ação do criminoso. O aprendizado comportamental é como qualquer outro. Envolve maturidade, experiência e instrução.

> Hackers tem encontrado uma forma de otimizar a eficiência da metodologia clássica ou do livro de receitas (cook-books). Os desenvolvimentos mais recentes mostram o uso de vírus e trojans como parte do modus operandi (Richard Stiennon da IT-Harverst).

As figuras 3.2 e 3.3 demonstram a anatomia hacker, como era e como é atualmente.

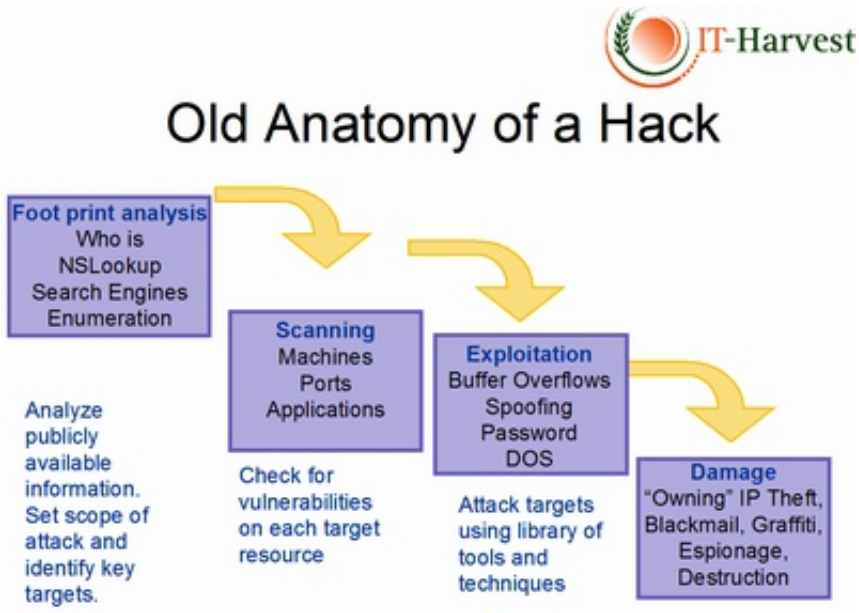

Figura 3.2: Antiga anatomia hacker (O'CONNOR, 2010)

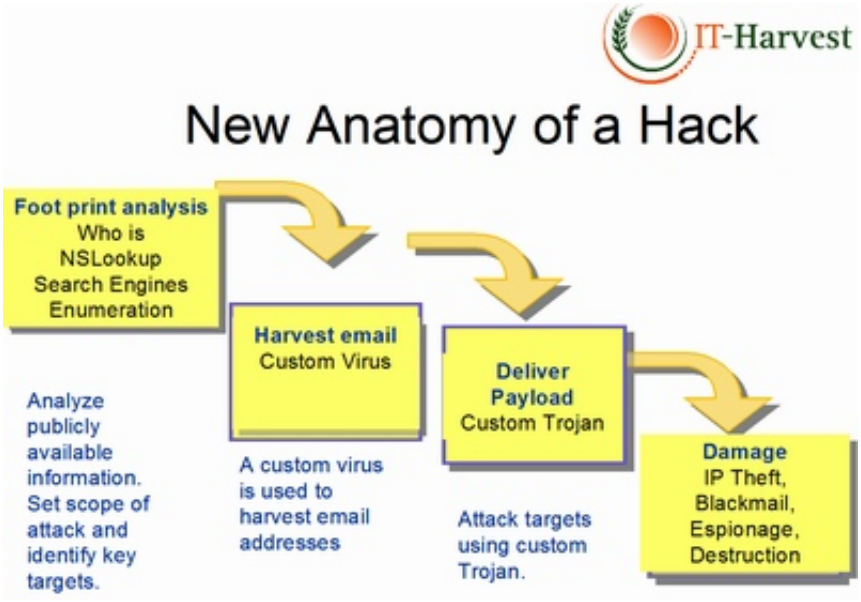

Figura 3.3: Nova anatomia hacker (O'CONNOR, 2010)

A diferença entre elas é que na nova anatomia o hacker se utiliza de vírus e trojans, desenvolvidos de forma costumizada, tendo este o mesmo efeito de alguém se infiltrar e instalar um keylogger ou um keystroke logger na máquina alvo. O novo método é considerado mais fácil e mais abrangente que o método antigo.

3.3 Estrutura do crime

Como foi analisado acima a anatomia dos ataques vai se modificando com o tempo. De forma parecida a estrutura para se cometer crimes online também evoluiu.

Antigamento o desenvolvedor do código malicioso era o mesmo que o disseminava e o que tinha a conta bancária preenchida com o montade dos furtos. Contudo essa abordagem se mostrou frágil e facilmente rastreável.

Hoje o crime trabalha de forma bem estruturada e especializada. Veja abaixo:

1. O desenvolvedor de códigos maliciosos apenas vende ou repassa gratuitamente o código;
2. O crimoso utiliza o código malicioso para capturar dados das vitimas por meio de spams e sites falsos;
3. O aliciador recruta laranjas para despistar o rumo do dinheiro furtado; e
4. O laranja fica na base desse piramide, sendo ele a posição mais delicada e perigosa.

3.3.1 Laranjas

> Esse cara é um acerola, pois vale por 10 laranjas
>
> Domingo Montanaro

No mundo do crime organizado existem dois tipos de laranja: o pessoa física e o pessoa jurídica.

No primeiro caso as pessoas são aliciadas para receberem montantes de dinheiro direto em suas contas bancárias e então fazerem transferências desse dinheiro para outras contas (que podem ser de laranjas). Em geral o laranja é aliciado por anúncios espalhados em sites legitimos como "Ganhe dinheiro sem sair de casa" (Figura 3.4) embolsando de 5% a 10% do valor furtado.

Figura 3.4: Anúncio para pegar laranjas(KASPERSKY, 2012)

Muitas vezes o laranja é o único a ir preso já que o mesmo não tem ideia de como funciona a cadeia crimosa e existem casos que ele nem sabe que faz parte de uma cadeia crimosa e é aliciado crendo que participa de uma atividade legal.

O laranja pessoa jurídica os criminosos abrem uma empresa e usam os cartões clonados pelos bankers e carders para comprar produtos e os vendem em lojas desconhecidas por preços muito a baixo do mercado, faturando e lavando o dinheiro no processo.

4 Prevenção

A prevenção visa impedir e ou inibir ações criminosas aos sistemas, tendo visibilidade maior onde o dano causado pode ser maior. A proteção se baseia em (TURBAN; MCLEAN; WETHERBE, 2004, p. 545-546):

- Prevenção;
- Detenção;
- Detecção;
- Limitação;
- Recuperação; e
- Correção.

É necessário agir preventivamente nesses pontos de atuação criminosa. Sistemas com fraca autenticação, o compartilhamento de senhas, a falta de rastreabilidade e vulnerabilidades de conectividade e mobilidade são os maiores motivadores para ocorrências de Cibercrime.

Existem diversas forças preventivas que inibem o ato criminoso digital, entre elas:

- Gestão de perfis;
- Monitoramento;
- Autenticação forte;
- Fortalecimento dos sistemas;
- Auditorias; e
- Fator Humano.

> Uma análise de custo-benefício mensurando a probabilidade de danos e perdas prováveis que poderiam ser combatidas com a implantação de um sistema de prevenção de fraudes deve ser considerada (BASTOS; PEREIRA, 2007a).

Alguns órgãos, tais como o FBI, disponibilizam dicas para evitar fraudes e também setores para combater fraudes cibernéticas (IC3, 2012). Essas dicas podem ser encontradas online disponíveis a todos que desejarem visualizá-las.

Também está disponível online um serviço para auxiliar na prevenção e combate a fraudes cibernéticas, o Monitor das Fraudes (PARODI, 2012) disponibiliza informações para identificação de fraudes, um decálogo antifraudes com dicas e sugestões para prevenção das mesmas.

Figura 4.1: (PARODI, 2012)

Existem atualmente inúmeras soluções que auxiliam na prevenção e no combate a fraudes cibernéticas. AntiSpams, AntiVirus, Firewalls, Controle de Acesso (Biometria, Leitura Ótica, etc.), Certificados Digitais.

4.1 Normas de Segurança

Diversos padrões foram desenvolvidos para melhorar a segurança das organizações, prevenindo e preparando a mesma para reagir ao incidente de forma coexa e rápida evitando ao máximo as perdas de ativos e de capital.

Inclusive em determinadas áreas as empresas devem está em conformidade a esses padrões, como é o caso do PCI[1] para empresas que lidam com transações de cartão de crédito.

[1] Payment Card Industry(PCI, 2012)

As normas da familia ISO 27000[2] foram desenvolvidas para abranger a segurança da informação como um todo e unificar boas práticas em um compilado em forma de normas guias. Já o COBIT[3] é um guia de boas práticas em forma de framework para gestão de TI.

É importante ressaltar que o em muitos casos a conformidade com as normas padrões da área não são obrigatórias, contudo são altamente recomendados e evitam ou atenuam diversas falhas ou quebras de segurança.

Como essas boas práticas foram feitas para otimizar o trabalho dos gestores, auditores e analistas de segurança, os mesmos quando bem implentados criam um ambiente fortimente protegido e com ampla capacidade de resposta a incidentes, mesmo que seja impossível garantir segurança total.

No âmbito forense as normas podem ajudar ao períto, assistênte técnico ou investigador a localizar desvios de conduta de funcionário ou encontrar eventos anormais no funcionamento de uma organização diminuindo o tempo e os recursos gastos para a ação.

4.2 Novos Desafios

Segue uma listas dos novos desafios:

- Inovação tecnológica.
- Engenharia social como fator humano.
- Técnicas avançadas de anti-forense e de evasão.
- Legislação.
- Colaboração internacional.

4.2.1 Inovação Tecnológica

Devido à grande velocidade da evolução tecnológica, de mídias, de dispositivos, de softwares e da própria velocidade da internet e inclusão digital, a tecnologia tem se tornado um grande desafio para os responsáveis pela segurança da informação.

[2](ISO, 2009)
[3](COBIT, 2012)

4.2.2 Engenharia Social

Acompanhando a tecnologia, um outro fator que sempre tem sido um grande desafio, com a facilidade de acesso às informações que é disponibilizada atualmente, o fator humado também é considerado como um grande desafio para a segurança da informação, tendo em vista ainda que sua fragilidade é utilizada em larga escala atualmente pelos cibercriminosos.

4.2.3 Técnicas Anti-Forense e de Evasão

As técnicas de anti-forense e de evasão cada vez mais avançadas, o uso de esteganografias, criptografia, etc.

4.2.4 Legislação

Necessidade de ajustes na legislação vigente para tipificar de melhor forma os crimes cibernéticos.

4.2.5 Colaboração Internacional

Colaboração e cooperação entre os órgãos de prevenção e combate aos crimes cibernéticos, agilizando os processos investigativos, mitigando a impunidade e a ocorrencia de novos incidentes.

5 *Questões Legais*

Hoje no Brasil não existe legislação específica para cibercrimes. Então os casos são tratados de modo geral pelo código penal[1] vigente de 1940 que não tinha condições de prevê os avanços tecnológicos que temos hoje tornando a tipicação dos crimes confusa e divergente.

O crime digital não é inpunível no Brasil, pelo contrário, mesmo sendo tendo uma legislação antiga datada da década de quarenta a mesma é genérica e ampla o suficiente para enquadrar em seus artigos muitos dos atos ilícitos cometidos por meios eletrônicos.

O crime digital pode acarretar em penas mais brandas do que os seus análogos não digitais. No caso de um assalto a banco o que o faz pessoalmente o assaltante é enquadrado em roubo com pena de quatro a dez anos além de poder imputar-lhe agravante de que pode aumentar a pena pela metade já a mesma quantidade de dinheiro roubado digitalmente incorre em furto simples onde a pena é de um a quatro anos e multa, já que ninguém pode "Subtrair coisa móvel alheia, para si ou para outrem, mediante grave ameaça ou violência a pessoa"[2] de um computador.

Para remediar isso existem alguns projetos de lei (PL) que pretendem suprir essa necessidade, como é o caso da PL 2793/11[3] que "Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências." que determina dentre outras coisas a pena de 3 meses a 1 ano pela invasão de computadores para obter, adulterar ou destruir dados que até a redação desse texto não tinha sido aprovada no senado. Além da famigerada Lei Azeredo[4] que também ficou conhecido AI-5 digital por artigos confusos e amplos em demasia.

[1] (PENAL, 1940)
[2] Art. 157 do Código Penal Brasileiro
[3] (TEIXEIRA, 2011)
[4] (PIAUHYLINO, 1999)

6 Combate

> Não há como combater as fraudes eletrônicas com eficiência sem comprometimento efetivo de provedores de internet, de email e de conteúdo, lan houses, cyber cafés e empresas de telecom, integrados em uma rede que deve reunir empresas, pessoas, autoridades e infraestrutura da sociedade digital (PINHEIRO, 2009).

Alguns órgãos contribuem no combate ao crime cibernético, reportando incidentes de segurança ocorridos. Um desses órgãos é o CAIS - Centro de Atendimento a Incidentes de Segurança. O mesmo tem a função informativa e educativa, exibe uma coleção de imagens de phishing scam e ou malwares veiculados por meio de spam.

Órgãos Nacionais que visam o combate do cibercrime:

- Ministério Público Federal (MPF);
- Policia Civil;
- DIG-DEIC - 4ª Delegacia de Repressão a Crimes de Informática de São Paulo (SP);
- DERCIFE (Delegacia Especializada de Repressão a Crimes contra Informática e Fraudes Eletrônicas), em Belo Horizonte (MG);
- DRCI - Delegacia de Repressão aos Crimes de Informática, no Rio de Janeiro (RJ), dentre outros.
- Policia Federal;
- Ccomgex - Centro de Comunicações e Guerra Eletrônica do Exército;
- SaferNet: Iniciativa privada;
- Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos: Inicialmente criado para combater crimes financeiros realizados pela rede, o centro foi ampliado para tratar das tentativas e ataques a sistemas de informação do governo federal [1];

[1] (GROSSMANN, 2012)

- Comissão de Direito eletrônico e crimes de alta tecnologia da OAB de SP;
- CDCiber - Centro de Defesa Cibernética; e
- CAIS - Centro de Atendimento a Incidentes de Segurança.

O combate ao cibercrime foi incorporado a órgãos no mundo inteiro, podemos citar com destaques em âmbito internacional:

- FBI (IC3 - Internet Crime Compliant Center); e
- Interpol.

Independente do órgão responsável, é bom salientar que o combate ao cibercrime deve vir a nível de Estado, tomando medidas como por exemplo:

- Políticas governamentais: legislação, polícias especializadas, departamentos de investigação etc;
- Cooperação entre órgãos;
- Ferramentas; e
- Informação: divulgação de informações entre as pessoas e presença da mídia.

7 *Visão de Produtos*

Atualmente existem diversas soluções no mercado voltadas diretamente ou indiretamente à prevenção, combate ou contenção de crimes realizados por meios digitais. Abaixo estão dispostas algumas dessas soluções para proteção e descontaminação de ambientes, controle de transações (e-commerce) e lavagem de dinheiro.

7.1 Soluções para Proteção/Descontaminação de Ambiente

Os softwares encontrados são os softwares mais utilizados na atualidade e em geral possuem um *"know-how"* e protegem os clientes com uma gama de sistemas especializados integrados [1] em uma solução completa.

- F-Security;
- Kaspersky;
- McAfee;
- Symantec;
- ESET; e
- CheckPoint.

Em geral, apesar dos softwares apresentarem diferentes fabricantes, ambos oferecem serviços similares de forma análoga e qualidade razoável.

[1] anti-virus, firewall, anti-spyware, etc

7.2 Segurança de Transações (e-commerce)

Esses sistemas visam maior controle transacional entre o cliente e o e-commerce, oferecendo garantias para ambas as pontas.

- SuperPay
- Paypal;
- CelarSafe;
- Mercado Pago;

7.3 Outros

O setor de anti-fraude é muito criativo e diariamente surgem diversas soluções ou pretensas soluções que visam a resolução de diversas fontes de fraudes, como por exemplo o *Wolters Kluwer - Banking Risk* com a promessa de evitar fraudes dentro da corporação (TOOLKIT, 2012).

7.4 Detalhe de Ferramentas

7.4.1 Symantec Endpoint Protection

O Symantec Endpoint (SYMANTEC, 2012b) Protection 12 combina o Symantec AntiVirus com uma prevenção avançada contra ameaças, visando fornecer uma defesa inigualável contra malware para laptops, desktops e servidores. Ele integra perfeitamente tecnologias de segurança essenciais em um único agente e console de gerenciamento, o que aumenta a proteção e ajuda a reduzir o custo total de propriedade.

Principais benefícios:

- Bloqueia malware como vírus, worms, Cavalos de Troia, spyware, adware, bots, ameaças de dia zero.
- Impede violações de segurança, o que reduz o custo administrativo.
- Reduz o custo total de propriedade para a segurança de endpoints.

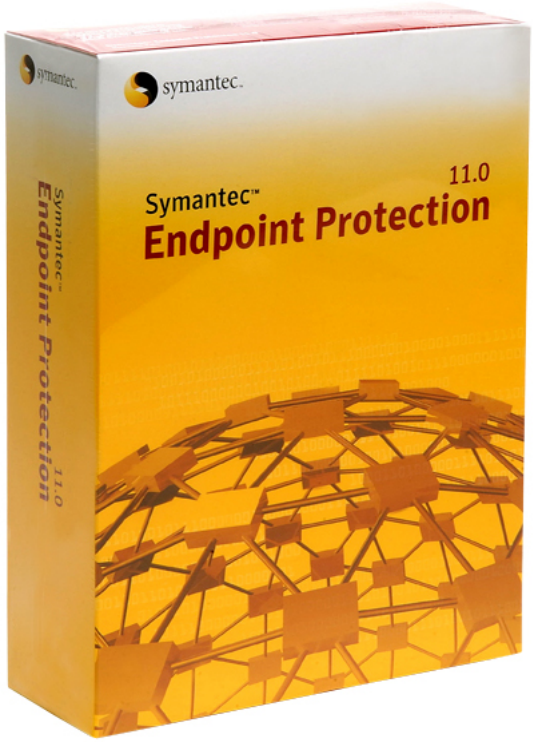

Figura 7.1: Sysmantec Endpoint Protection (SYMANTEC, 2012b)

Agentes

Oferece um único agente para todas as tecnologias do Symantec Endpoint Protection e do Symantec Network Access Control. Oferece uma única interface integrada para o gerenciamento de todas as tecnologias do Symantec Endpoint Protection e do Symantec Network Access Control. Tudo isso permite um único método de comunicação e sistema de entrega de conteúdo em todas as tecnologias. Garante eficiência operacional, como atualizações únicas de software e de políticas.

Centraliza e unifica a criação de relatórios. Oferece manutenção e licenciamento unificados. Não é necessário efetuar mudanças no cliente ao acrescentar enforcement do Symantec Network Access Control.

Console da Web com login único

Gerencia ambiente de forma eficiente através de um console da Web com login único, que fornece aos administradores gerenciamento total das configurações, geração de relatórios e exibições de painéis consolidados em diferentes tecnologias de proteção da Symantec.

- Gerenciamento fácil;

- Gerenciamento e administração unificados;
- Remove soluções existentes, instala novos clientes e cria relatórios sobre eles automaticamente. Gerencia clientes Windows e Mac pelo mesmo console.

Controle de aplicativos

Permite que os administradores controlem o acesso de usuários e de outros aplicativos a processos, pastas e arquivos específicos. Oferece análise do aplicativo, controle de processos, controle de acesso ao registro e arquivo, bem como controle de DLL e módulo. Permite que os administradores restrinjam determinadas atividades consideradas suspeitas ou de alto risco. Impede que malware se propague ou danifique os endpoints. Bloqueia os endpoints para evitar vazamento de dados.

Controle de dispositivos

Controla quais periféricos podem ser conectados ao computador e como eles são usados. Bloqueia endpoints para impedir a conexão de unidades ”thumb”, gravadores de CD, impressoras e outros dispositivos USB. Evita que dados confidenciais e importantes sejam extraídos ou roubados dos endpoints (vazamento de dados).

Evita que os endpoints sejam infectados por vírus provenientes de dispositivos periféricos.

Análises e relatórios avançados

O Symantec Endpoint Protection agora inclui o Altiris IT Analytics Symantec Endpoint Protection Pack. O ITA complementa e expande o relatório tradicional oferecido pelo Symantec Endpoint Protection, através da incorporação de uma análise multidimensional e relatórios gráficos robustos, em um painel fácil de usar.

Symantec Protection Suite

O Symantec Protection Suite cria um ambiente de endpoints e mensageria protegido contra as complexas ameaças atuais, como malware, perda de dados e spam, e pode ser rapidamente recuperado no caso de falhas (CISCO, 2012d). Ele reduz os custos de proteção do seu ambiente e gerencia de forma mais eficaz os riscos inerentes às infra-estruturas atuais de TI.

Desvantagens

Como qualquer software o Symantec oferece algumas desvantagens(ROCHA, 2008) como:

1. DHCP: Os computadores clientes de redes SBS não conseguem receber endereços de IP, via DHCP, mas se o IP for determinado manualmente funciona tudo de forma normal; e
2. Acesso às pastas compartilhadas: os computadores clientes perdem a conexão com as pastas compartilhadas após um determinado período de tempo. Apenas rebootando o servidor este problema é resolvido.

Este problemas foram documentados no (SYMANTEC, 2012a). Existe também um documento disponibilizado pela Symantec que resolve o problema das pastas inacessíveis (TECH102742, 2012).

7.4.2 Cisco NAC Agent

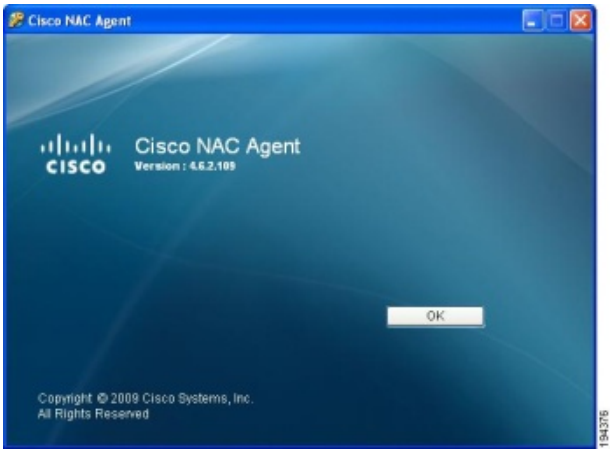

Figura 7.2: Cisco NAC Agent (CISCO, 2012b)

NAC (Network é uma das opções tecnológicas disponíveis para a verificação e atualização dos sistemas antes de seu ingresso efetivo na rede. É um sistema de controle de acesso à rede com funcionalidades para:

- Integrar a autenticação do usuário;
- Gerenciar o acesso às informações da rede;
- Gerenciar a "saúde" da máquina com proteção contra ameaças;
- Controle de acesso baseado nas políticas da rede da organização;

Autenticação

Autenticação é usada para verificar uma identidade alegada junto à rede para que o acesso seja liberado ou negado.

Autorização

Conceito de associar diferentes serviços aos usuários após a autenticação.

Validação

É verificado se está de acordo com as políticas estabelecidas pelo departamento de TI e se atende aos requisitos de verificação de patches atualizados, assinaturas de antivírus, serviços e aplicações ativas.

Quarentena (Depende da política do NAC)

Quando o dispositivo não está em conformidade com as políticas da organização o acesso à rede é bloqueado ou vai para reparo.

Reparo

Se o controle de acesso à rede é robusto, após ser redirecionado para um servidor de quarentena, o computador cliente passará por um reparo de acordo com as políticas pré-definidas:

- Atualização das assinaturas de antivírus;
- Atualização dos patches do sistema operacional;
- Limpeza de malwares detectados;
- Desativação de serviços desnecessários.

A inspeção é uma das principais funções da arquitetura NAC e a avaliação ocorre de acordo com a eficiência do sistema de prevenção de intrusão (IDS/IPS) adotado.

Figura 7.3: Servidor Cisco NAC (CISCO, 2012b)

Servidor Cisco NAC

Como NAC Funciona

A figura abaixo representa o funcionamento da NAC (CISCO, 2012a).

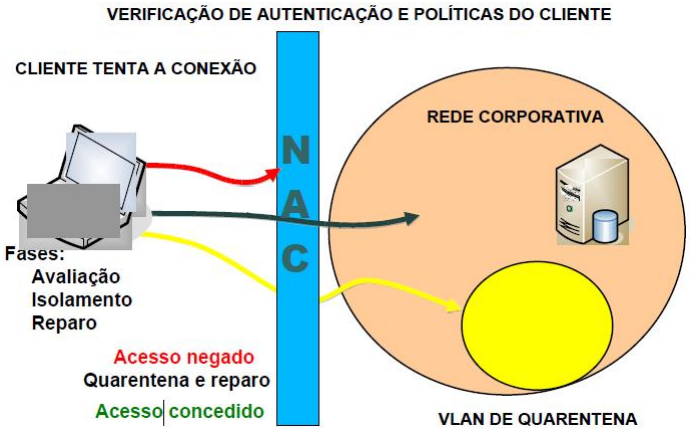

Figura 7.4: Funcionamento do Cisco NAC (CISCO, 2012c)

Desvantagens

A rede coorporativa deve estar sempre bem estruturado com o servidor e alinhado informações com os analistas dos servidores pois qualquer descuido pode ocasionar lentidão extrema da rede e impossibilitar acessos de usuários no qual estão ativos.

7.4.3 Check Point

Check Point oferece versão Media Encryption e Protector Client que protege os dados confidenciais criptografando todas as informações dos equipamentos como notebooks e desktops

Figura 7.5: Check Point (POINT, 2012a)

coorporativos bloqueando invasão de malvaware ou prevenção de cópia de qualquer informação contida no equipamento. Além de criptografar mídia de HD Hard Disc (disco rígido), Check Point bloqueia acessos como dispositivos de armazenamento USB, CDs e DVDs e controlar a atividade (ler, escrever e executar) nas portas e dispositivos. Todo o conteúdo do dispositivo é automaticamente codificado em segundo plano para uma experiência transparente ao usuário final.

A criptografia Check Point Full Disk Encryption simplifica a implementação e gerenciamento de segurança de endpoint ao criptografar automaticamente todo o conteúdo do disco rígido, inclusive o sistema operacional e arquivos de sistema existentes, temporários e apagados. Este novo nível de proteção protege as empresas de acesso não autorizado a informações corporativas ou ataques de rede, mesmo se o disco rígido for fisicamente transferido para outro computador. Possibilita aos clientes protegerem diversos sistemas operacionais, aperfeiçoando significativamente a implementação e uso de criptografia de disco completo em ambientes mistos. O Check Point Full Disk Encryption também oferece recursos centralizados de implementação, gerenciamento e registro de eventos (logging), para simplificar a administração de políticas de segurança, dinamizar a conformidade e reduzir o custo total de propriedade. O Check Point Full Disk Encryption é adaptável para qualquer organização e foi testado em implementações em grandes indústrias e repartições públicas em todo o mundo. Além disso, o Check Point Full Disk Encryption foi premiado com as mais importantes certificações de segurança - inclusive International Common Criteria EAL4, FIPS-140-2 e BITS - possibilitando assim rápida conformidade com regras e regulamentações globais de privacidade de dados. Não importa que sistemas operacionais estejam em uso nas suas redes, os clientes beneficiam-se de tecnologia poderosa de criptografia e segurança de dados da Check Point. A estabilidade e flexibilidade do Check Point Full Disk Encryption são benefícios essenciais para gerenciar facilmente nosso ambiente de trabalho sem comprometer o nível de segurança no endpoint para qualquer sistema operacional em funcionamento (POINT, 2012b).

Podemos agora compartilhar informações sem dificuldades, sabendo que os dados de nos-

sos clientes estão seguros.

- Autenticação Pré-Inicialização que requer nome de usuário e senha antes que o sistema operacional seja carregado, elevando a segurança. O Check Point Full Disk Encryption também permite autenticação multifatores, como Smart Cards ou tokens baseados em certificações;
- Ajuda Segura Remota dá aos usuários opções de ajuda remota e suporte remoto baseado na web para tokens e senhas de acesso perdidos;
- A Interface Única de Usuário simplifica a instalação, administração e fácil integração, suporta diversas linguagem para implementações globais. A operação automática e transparente tem efeito mínimo sobre a produtividade dos usuários finais; e
- Gerenciamento Central e Registro de Eventos permitem fiscalização central de políticas de seguranças para atender as crescentes necessidades de conformidade. O gerenciamento central de configuração reduz o custo total de propriedade.Nota: As informações foram fornecidas pela Check Point.

Desvantagens

Dependendo da quantidade de informações o processo de criptografia pode ser demorado.

O equipamento apresentando problemas no sistema operacional ao efetuar o backup o analista deve conter em mãos o CD de descriptografia caso contrário o mesmo deve solicitar ao suporte checkpoint o CD no qual esse processo é um pouco demorado e burocrático.

7.4.4 Outras Ferramentas

OTP (One Time Password)

Ferramenta composta de senha de uso único. Utiliza complexos algoritmos criptográficos unidirecionais com base em um número aleatório. “Uma forma de identificação do usuário em determinados ambientes. A solução tem três modalidades difundidas: sincronismo por evento - senhas geradas a partir de uma função recursiva que utiliza a semente e o último número gerado; por tempo - sincronização ente dispositivo e servidor; ou desafios/respostas onde a senha é gerada com base na semente e um desafio (número) informado pelo servidor.” (Julio Graziano Pontes - Gerente de Serviços da True Access)

CPQD (Gestão Integrada de Fraudes e Eventos)

Voltada para a prevenção de fraudes em transações bancárias, apoia a monitoração e a investigação on-line e em tempo real, de forma pró-ativa, de transações monetárias e não monetárias realizadas por meio dos diversos canais de relacionamento. A solução do CPqD promove uma completa integração entre: core bancário (autorizadores), eventos e incidentes de segurança e o tratamento de transações suspeitas.

ACI Proactive Risk Manager (SYSTEMS, 2012)

Solução abrangente de gerenciamento de crime financeiro, uma solução para auxiliar emissores de cartões, comerciantes e compradores a combater a fraude das instituições financeiras e esquemas de lavagem de dinheiro.

Figura 7.6: Proactive Risk Manager for Enterprise Risk

CanIt AntiSpam (UNODATA, 2012)

O CanIt é uma poderosa ferramenta de combate a spam, vírus e fraudes eletrônicas utilizado por importantes empresas brasileiras. Dentre os clientes, destacam-se inúmeros provedores de internet como America-Net, Netlink, BitcomNet, diversas instituições de ensino como Universidade de Brasília, FMU, Universidade Federal de Pernambuco, UFPE, Universidade Federal de Viçosa, Universidade Federal de Itajubá, Unesp, além de TV Cultura, Berkley International, entre outras. Compatível com sistemas Microsoft Exchange, Lotus Notes, Linux Based, atende a corporações desde 5 até milhões de caixas postais.

Figura 7.7: CanIt AntiSpam

8 *Case de sucesso*

8.1 OTP (One Time Password) com integração ao Connectra da Check Point

A implementação da ferramenta em conjunto assegurou uma segurança maior e resultou na redução à quase zero da incidência de fraudes.

A companhia implementou essa ferramenta em uma rede de loja varejista que comercializava seus produtos e serviços através de canais de venda distribuídos pelo Brasil. Os sistemas de frente de caixa e retaguarda eram disponibilizados aos canais pela web, o que havia alto índice de fraudes. “O grande problema nesse caso era o compartilhamento de senhas e a gestão desse ambiente”.

“Foi usada a integração do Connectra com o OTP para proporcionar autenticação segura com custo baixo. Também foi implementado um sistema de gestão de identidades para sincronizar os contratos do lojista e conceder os acessos em tempo real.

Nosso cliente tem acesso a uma página na web onde estão os aplicativos e essa pagina baixa um script que verifica a segurança da estação. Em um segundo momento, o usuário envia as credenciais (conta e senha) mais a OTP, onde é garantida a segurança de quem está acessando estabelecendo um canal seguro. Com o OTP conseguimos integrar as aplicações com efeito na execução e combate a fraudes, roubo de senhas foram evitados nesse processo” (Julio Graziano Pontes - Gerente de Serviços da True Access)

9 *Recuperação de Perdas*

9.1 Impacto de Fraudes Financeiras

Para (BASTOS; PEREIRA, 2007a, p. 04), a fraude eletrônica é um grande desafio para o setor financeiro.

> Segundo (CAMARGO, 2005, p. 02) a auditoria de sistemas em "e-business" e fraudes eletrônicas é um dos maiores desafios da fiscalização do sistema financeiro. O aumento substancial das negociações via internet, conforme destacado pela pesquisa da Federação Brasileira dos Bancos (FEBRABAN), segundo a qual as transações por "internet banking P.F." cresceram 450% entre 2000 e 2004, é a maior causa do crescimento deste tipo de auditoria. A instantaneidade dessas negociações via cartão de crédito impacta em maiores riscos de fraudes, pois muitas das vezes tais negociações são autorizadas sem a efetiva participação, ou seja, presença do cliente.

Atualmente, Eduardo Chedid, vice-presidente executivo de produtos e negócios da Cielo, a cada R$ 100 gastos em compras, R$ 0,75 (figura 9.1 são fraudados (BASTOS; PEREIRA, 2007b), ou seja, a realidade apresentada em 2007 por (BASTOS; PEREIRA, 2007a) continua presente.

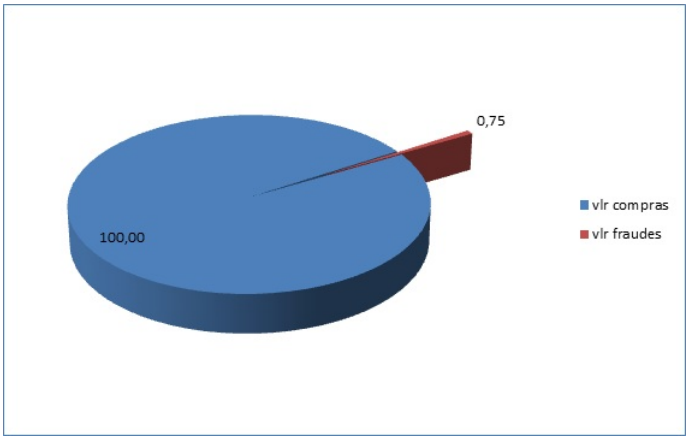

Figura 9.1: Fraudes em Transações Eletrônicas

O Brasil movimentou mais de 670 bilhões de reais em transações de cartões (operações de

débito e crédito) em 2011 (PETRY, 2012). Isso representa mais de 5 bilhões de reais seriam desprendidos somente com fraudes eletrônicas.

Em pesquisa do Norton (SYMANTEC, 2012c) o e-crime chega a movimentar mais de US$114 bilhões e as empresas gastam mais cerca de US$274 bilhões com reparações, juntos somam US$388 bilhões de prejuizos no total.

Dados apontam que o crime tradicional está migrando em grande escala para o mundo virtual, segundo noticia da Adrenaline (ADRENALINE, 2011):

> Em 2010, foram R$900 milhões roubados através de golpes online, contra "só" R$55 milhões do crime tradicional. E a tendência é de aumentar, e muito: apenas na primeira metade deste ano, foram R$685 milhões desviados via Internet.

Em pesquisa da Symantec (SYMANTEC, 2011), além do impacto financeiro o roubo de informações pessoais gerou um dos maiores impactos com perdas sofridas pelo cibercrime.

Figura 9.2: Perdas sofridas(SYMANTEC, 2011)

9.2 Cálculo das Chances de Recuperação de Perdas

Questionário de probabilístico de recuperação de perdas com fraudes. É um serviço que visa estimar a probabilidade de se recuperar uma parte consistente das perdas. Também estima a oportunidade de iniciar uma ação de recuperação através de uma empresa de recuperação de perdas por fraudes. Obviamente, o serviço é indicativo, sendo necessária uma análise mais profunda em cada caso para se obter um parecer mais confiável.

Figura 9.3: Custos do ciberataque(SYMANTEC, 2011)

9.3 Procedimentos para Recuperação de Perdas

A recuperação de perdas por uma empresa é um processo quase sempre problemático. Por tal motivo deve ser administrado por especialistas. Muitos golpes apresentam traços comuns dos criminosos, a preocupação em ocultar sua verdadeira identidade, rapidez e eficiência em desaparecer com os bens furtados.

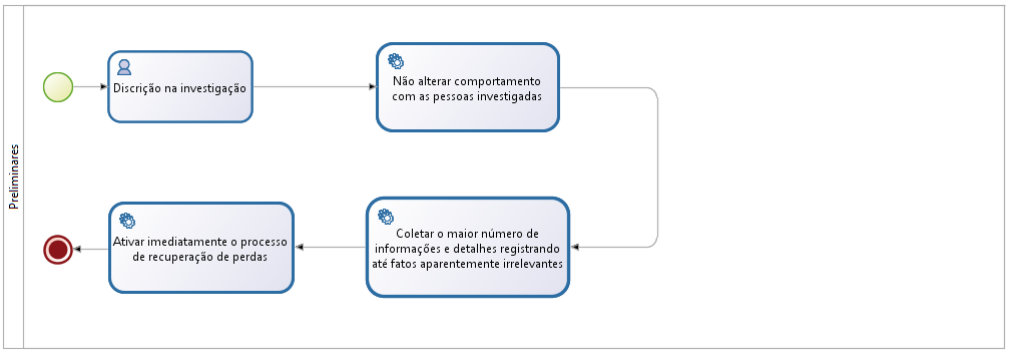

Figura 9.4: Preliminares ao Processo de Recuperação

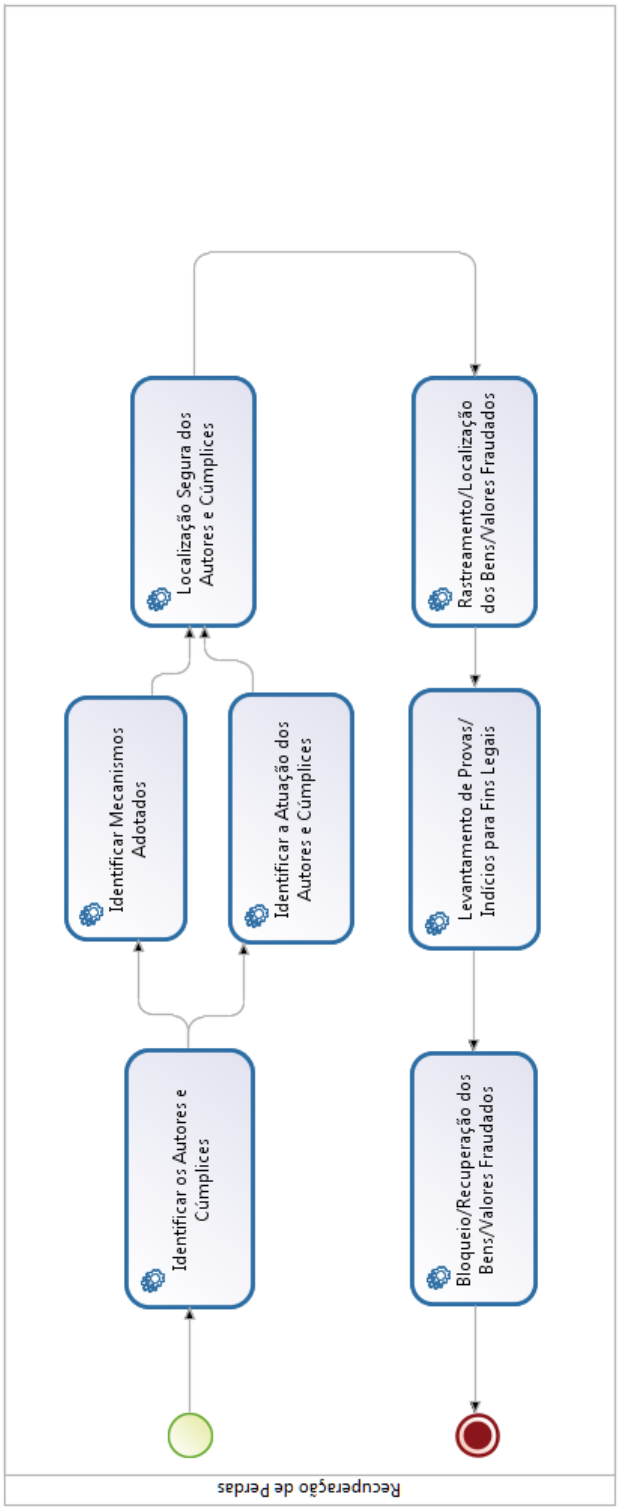

Figura 9.5: Processo de Recuperação

10 Conclusão

Como podemos ver ao longo do documento o cibercrime[1] tem diversas facetas e muda constantemente. Dentro deste, a fraude é um dos principais crimes cometidos e tem como maior vetor o phishing, inclusive foi apresentado um caso recente que chamou a atenção da mídia recentemente [2].

Nesse problema mundial de fraudes, o Brasil se destaca negativamente ao liderar o *ranking* dos maiores produtores e utilizadores de *banker* do mundo e que ao contrário do que se possa esperar a maioria dos ataques feitos são realizados por pessoas com pouco conhecimento técnico que se utilizam de *receitas de bolos*[3] para a prática do ilícito.

Podemos analisar a estrutura atual do crime organizado e como o processo funciona aliciando laranjas para mascarar o dinheiro furtado. Analisamos questões legais e chegamos a discursão sobre prevenção e combate ao cibercrime em diversos aspectos e seus novos desafios. Mostramos a reação do mercado com seus produtos e soluções comerciais. Por fim mostramos o estrago que o cibercrime causa na economia.

[1] é todo crime onde o computador é o principal meio para cometê-lo
[2] Caso Carolina Dieckmann
[3] Códigos maliciosos de terceiros

Referências Bibliográficas

ADRENALINE. *Brasil lidera criação de vírus que roubam dados bancários*. 2010. Disponível em: <http://adrenaline.uol.com.br/seguranca/noticias/6046/brasil-lidera-criacao-de-virus-que-roubam-dados-bancarios.html>.

ADRENALINE. *Como funciona o cibercrime brasileiro*. 2011. Disponível em: <http://adrenaline.uol.com.br/seguranca/artigos/162/como-funciona-o-cibercrime-brasileiro.html>.

BASTOS, P. S. S.; PEREIRA, R. M. Fraudes eletrÔnicas: O que hÁ de novo? 2007. Disponível em: <http://www.sergiomariz.com/mcc.uerj/index2.php?option=com_docman&task=doc_view&gid=20&Itemi

BASTOS, P. S. S.; PEREIRA, R. M. Fraudes eletrÔnicas: O que hÁ de novo? 2007.

CAMARGO, F. *Fraudes eletrônicas assustam setor financeiro*. 2005. Disponível em: <http://webinsider.uol.com.br/imprimir.php?id=2045>.

CARPANEZ, J. *Conheça os crimes virtuais mais comuns*. 2012. Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u19455.shtml>.

CARTãO, V. Y. B. dos. *Video Youtube: Bonde dos Cartão*. 2012. Disponível em: <http://www.youtube.com/watch?v=XXnQgv9F0yc>.

CERT.BR. *Núcleo de Informação e Coordenação do Ponto BR*. 2012. Disponível em: <http://www.cert.br/>.

CISCO. *Cisco NAC Appliance Agents*. 2012. Disponível em: <http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/461/cam/m_webagt.html>

CISCO. *CISCO Web site*. 2012. Disponível em: <www.cisco.com>.

CISCO. *Implementing Network Admission Control*. 2012. Disponível em: <http://i.i.com.com/cnwk.1d/i/tr/downloads/home/1587052539_chapter_6.pdf>.

CISCO. *NAC Solution And Technology Overview*. 2012. Disponível em: <http://www.informit.com/content/images/1587052253/samplechapter/1587052253ch1.pdf>.

COBIT. *COBIT 5*. [s.n.], 2012. Disponível em: <https://www.isaca.org/COBIT/pages/default.aspx>.

GIL, A. de L. *Fraudes Informatizadas*. 2ª. ed. São Paulo: Atlas, 1991.

GROSSMANN, L. O. *Crimes cibernéticos: Polícia Federal faz teste de larga escala com Rio+20*. 2012. Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=30670&sid=18>.

IC3. *Internet Crime Complaint Center*. 2012. Disponível em: <http://www.ic3.gov/default.aspx>.

ISO. *ISO 27000*. 2009. Disponível em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=41933>.

KASPERSKY. *Kaspersky*. 2012. Disponível em: <kaspersky.com>.

MACHADO, M. P.; ELEUTÉRIO, P. M. da S. *Desvendando a Computação Forense*. [S.l.]: Novatec, 2011. ISBN 978-85-7522-260-7.

O'CONNOR, T. *THE MODUS OPERANDI OF HACKING*. 2010. Disponível em: <http://www.drtomoconnor.com/3100/3100lect04.htm>.

PARODI, L. *Monitor das Fraudes*. 2012. Disponível em: <http://www.fraudes.org/>.

PCI. *PCI*. 2012. Disponível em: <https://www.pcisecuritystandards.org/>.

PENAL, C. *Código Penal*. Rio de Janeiro: [s.n.], 1940. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>.

PETRY, R. *Débito deve ultrapassar cartão crédito em 2012*. 2012. Disponível em: <http://blogs.estadao.com.br/jt-seu-bolso/tag/associacao-brasileira-das-empresas-de-cartoes-de-credito-e-servicos/>.

PIAUHYLINO, L. *PL 84/1999*. 1999. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=15028>.

PINHEIRO, P. P. *Como prevenir e combater a fraude eletrônica?* 2009. Disponível em: <http://www.partnersales.com.br/artigo/48/como-prevenir-e-combater-a-fraude-eletronica>.

POINT, C. *Check Point Full Disk Encryption*. 2012. Disponível em: <http://www.checkpoint.com/products/full-disk-encryption/index.html>.

POINT, C. *Security Gateways*. 2012. Disponível em: <http://www.layer8-it.net/l8/index.php/sv/checkpoint-security>.

ROCHA, C. F. P. da. *Problemas com o Symantec Endpoint Protection 11.0*. 2008. Disponível em: <http://carlosfprocha.com/blogs/paleo/archive/2008/02/08/problemas-com-o-symantec-endpoint-protection-11-0.aspx>.

RODRIGUES, R. *Brasil é líder em vírus que roubam dados bancários, diz pesquisa*. 2012. Disponível em: <http://idgnow.uol.com.br/seguranca/2010/08/24/brasil-e-lider-em-virus-que-roubam-dados-bancarios-diz-pesquisa/>.

RODRIGUES, R. *Quer ser um cibercriminoso? Crackers brasileiros agora oferecem curso online*. 2012. Disponível em: <http://idgnow.uol.com.br/seguranca/2012/01/17/quer-ser-um-cibercriminoso-crackers-brasileiros-agora-oferecem-curso-online/>.

SCHWEITZER, D. *Incident Response: Computer Forensics Toolkit*. [S.l.]: Wiley, 2003. ISBN 9780764526367.

SYMANTEC. Relatório sobre segurança da informação nas empresas. 2011.

SYMANTEC. *FAQ Customer Installations Issues with Resolutions*. 2012. Disponível em: <http://www.symantec.com/business/support/endpointsecurity/sep11_faq_customer-installations-issues-with-resolutions_int_112007%20partner(3)).pdf>.

SYMANTEC. *Symantec Web Site*. 2012. Disponível em: <http://www.symantec.com/pt/br/>.

SYMANTEC, N. *Norton Cybercrime Report: The Shocking Scale of Cybercrime*. 2012. Disponível em: <http://uk.norton.com/cybercrimereport/promo>.

SYSTEMS, A. P. *ACI Proactive Risk Manager*. 2012. Disponível em: <http://www.aciworldwide.com/en/Products-and-services/Payments-fraud/Fraud-detection-and-AML/Proactive-Risk-Manager.aspx>.

TECH102742. *Windows Servers stop accepting network connections with Symantec Endpoint Protection 11.0 installed*. 2012. Disponível em: <http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007102613484948>.

TEIXEIRA, P. *PL 2793/2011*. 2011. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=529011>.

TOOLKIT, B. O. *Anti-Fraud Software Solutions*. 2012. Disponível em: <http://www.toolkit.com/small_business_guide/sbg.aspx?nid=P14_3230>.

TURBAN, E.; MCLEAN, E.; WETHERBE, J. *Tecnologia da Informação para Gestão: Transformando os Negócios na Economia Digital*. 3ª. ed. São Paulo: Bookman, 2004.

UNODATA. *AntiSpam and Internet Solutions*. 2012. Disponível em: <http://www.unodata.com.br/software_antispam>.

WIKIPÉDIA. *Crime informático*. 2012. Disponível em: <http://pt.wikipedia.org/wiki/Crime_informático>.