POLÍCIA CIVIL DE SÃO PAULO

“Cibercrimes: Uma Ameaça Atual e Efetiva”

Cenário atual das ameaças cibernéticas no meio corporativo.

INTRODUÇÃO:

A utilização da tecnologia pelos criminosos tem sido um dos maiores desafios para os órgãos de investigação na atualidade.

Principais desafios no combate aos cibercrimes:

- A imensa complexidade do mundo da informação no século 21;
- Expansão contínua e em escala mundial da internet;
- Número crescente de dispositivos móveis;
- Multiplicação das fontes de informações, no fenômeno chamado Big Data.
- Necessidade contínua da revisão e atualização da segurança eletrônica de todas as empresas permanentemente.

O novo cenário da criminalidade:
Cibercrime:

Crime que pode ser promovido de diversas maneiras: disseminação de vírus que coletam e-mails para venda de mailing; distribuição de material pornográfico (em especial infantil); fraudes bancárias; violação de propriedade intelectual e direitos conexos ou mera invasão de sites para deixar mensagens difamatórias como forma de insulto a outras pessoas ou para furtar informações.

O termo "cibercrime" surgiu depois de uma reunião, em Lyon, na França, de um subgrupo das nações do G8, que analisou e discutiu os crimes promovidos via aparelhos eletrônicos ou pela disseminação de informações para a internet. Isso aconteceu no final da década de 90, período em que Internet se expandia pelos países da América do Norte.

Alguns conceitos para Cibercrimes:

O manual das Nações Unidas para Prevenção e Controle dos Crimes por Computador define os crimes de computador como sendo:

- **(1) fraude por manipulação do computador;**
- **(2) falsificações por computador;**
- **(3) danos ou modificações de dados ou programas de computador;**
- **(4) acesso não autorizado a sistemas e serviços de computador;**
- **(5)reprodução não autorizada de programas legais de computador;**

Alguns conceitos para Cibercrimes:

A Convenção de Budapeste define nos artigos 2 a 10 o cibercrime, estabelecendo conteúdo de matéria penal em quatro diferentes categorias:

- **(1) infrações contra a confidencialidade, a integridade e a disponibilidade de dados e sistemas;**
- **(2) As infrações relacionadas com computador;**
- **(3) infrações relacionados com conteúdo;**
- **(4)delitos relacionados com a violação dos direitos de autor e direitos conexos.**

Momento atual:

Apesar da recessão global, da segurança aprimorada e das medidas punitivas internacionais, o cibercrime cresceu a uma taxa de dois dígitos ano após ano nessa última década.

Momento atual:

Até 2021, o custo do cibercrime deve chegar a US$ 6 trilhões por ano – um valor 15 vezes maior do que o registrado em 2015, de US$ 400 bilhões.

A previsão é da empresa de pesquisa em cibersegurança “Cybersecurity Ventures”.

Os gastos incluem danos aos dados, perda de produtividade, furto de propriedade intelectual, de dados pessoais e financeiros, fraudes, interrupção de processos de negócio, investigações forenses, restauração e deleção de dados e sistemas infectados e danos à reputação.

Sete principais ações do cibercrime nos últimos anos:

1. A infecção em massa do worm “MyDoom”: danos estimados em US$ 38 bilhões.
2. “ O falso afeto do worm “I LOVE YOU”: danos estimados em US$ 15 bilhões.
3. Destruição furtiva do “worm” Conficker: danos estimados em US$ 9,1 bilhões.
4. “Worm” Stuxnet — Agressivo e perigoso: dano desconhecido.
5. Rede de bots Zeus — Um ladrão de informações versátil: dano desconhecido.
6. “Duqu” malware sofisticado e totalmente customizado: dano desconhecido.
7. Flame um vírus feito para ser capaz de tirar screenshots das máquinas dos usuários, monitorar conversas baseadas em voz, ter (e responder) complexas instruções remotas e fazer o “sniffing” do tráfego da web enquanto o usuário navega na Internet, além de sequestrar contas administrativas e detectar qual software antivírus está instalado.

O que motiva a prática dos cibercrimes?

- Obtenção de ganhos financeiros fáceis;
- Necessidade de provar a capacidade em vencer o computador ou a empresa;
- Competição tecnológica;
- Revolta ou vingança contra a empresa, normalmente funcionários demitidos;
- Motivações ideológicas, políticas ou religosas por pessoas que desejam fazer chantagem, invadir sistemas secretos ou de segurança e provocar terrorismo ou catástrofes.
- Cyberwar

Perspectivas quanto aos cibercrimes no mundo:

Segundo Arthur Coviello Jr., presidente da RSA, divisão de segurança da empresa norte-americana EMC e um dos maiores especialistas em segurança eletrônica, o mundo não poderá vencer o cibercrime ou crime cibernético sem a associação de quatro estratégias: educação, administração de riscos, compartilhamento de informações e ações de governo. Se a guerra não ocorrer nessas quatro frentes, os resultados serão sempre medíocres.

Perspectivas quanto aos cibercrimes no mundo:

No que diz respeito ao combate as ameaças do mundo virtual, o mundo não poderá vencer o cibercrime sem a associação de quatro estratégias: educação, administração de riscos, compartilhamento de informações e ações de governo. Se a guerra não ocorrer nessas quatro frentes, os resultados serão sempre medíocres.

Dificuldades para descobrir os crimes por computador:

- Distância temporal: porque normalmente são crimes continuados, cometidos por muito tempo, e muito da documentação e arquivos são expurgados, não tendo como ser descoberta a fraude;
- Distância espacial: o indivíduo pode iniciar o crime num local e o cúmplice o termina em outro local. É o caso de emissão de ordens de pagamento falsificadas;
- Prejuízo elevado, difícil de avaliar;
- Pouco conhecimento na área.

Outras dificuldades encontradas:

- Técnicas:
- Disseminação do uso da criptografia
- Grande dimensão dos discos rígidos
- Smarts cards e drives
- Senhas biométricas
- Política
- Investimento estatal na investigação com aparelhamento das unidades especializadas, perícia e treinamento policial = quase 0,
- na contra-mão dos caminhos adotados pela criminalidade

Dificuldades para se punir quem pratica crimes por computador :

- falta de previsão legal específica;
- empresa acaba não denunciando o criminoso por medo de perder a credibilidade perante os clientes;
- a empresa acaba perdoando o criminoso desde que este revele como entrou no sistema e "qual a falha" para evitar futuras invasões;
- é difícil a obtenção de provas do crime;
- são necessárias muitas testemunhas;
- é um processo lento e muito oneroso.

Tendências mundiais no combate aos cibercrimes:

Padronização da Coleta de Informações

A forma como um indício ou prova são recolhidos depende do crime cometido e do tempo em que tenha se consumado. Se um crime já foi cometido, o computador é simplesmente apreendido, e é feita uma tentativa de coleta de dados. Se um crime está em andamento, no entanto, será necessária a instalação de ferramentas para controle de atividades realizadas no computador e coleta de indícios e provas. Unidades de investigação do mundo todo estão adotando protocolos de investigação que primam pelo efetivo controle das atividades realizadas em um computador e preservação de indícios e provas, padronizando seus procedimentos para evitar metodologias conflitantes.

Tendências mundiais no combate aos cibercrimes:

Aumento na destinação de recursos

Unidades policiais especializadas em cibercrimes devem acompanhar a tecnologia atual, de forma a estarem em constante aperfeiçoamento. Seus integrantes devem ser treinados em todas as novas tecnologias e deve ser exigido dos mesmos uma constante evolução e aperfeiçoamento. Cada investigador deve ser um especialista em informática forense e encontrar-se apto a identificar e coletar indícios e provas, sendo necessário que suas atividades estejam na mais absoluta sincronia com o trabalho realizado por peritos forenses, com os quais em hipótese nenhuma devem ser confundidos.

Tendências mundiais no combate aos cibercrimes:

Articulação de unidades de investigação.

As unidade policiais que investigam cibercrimes nem sempre se entendem sobre quem é o responsável pela investigação deste tipo de delito e nem trocam informações. Investigação de cibercrimes envolve conhecimentos especiais por parte dos agentes envolvidos e recursos muito mais específicos do que aqueles disponíveis em investigações comuns. Unidades policiais do mundo todo estão adotando modelos de investigação que implicam na especialização de suas unidades e principalmente na articulação de todos os órgãos envolvidos na investigação destes crimes, sempre compartilhando recursos.

Tendências mundiais no combate aos cibercrimes:

Toda a Legislação sobre cibercrimes deve estar sempre em revisão e a cooperação entre os países deve ser aperfeiçoada.

Diante do avanço tecnológico constante e da expansão das redes de computadores por todo o mundo, os países devem ter uma preocupação constante sobre a troca de informações entre eles e a eficácia de suas leis no combate aos cibercrimes, visando sempre reprimir de forma uniforme crimes que podem assumir um caráter transnacional como é o caso dos cibercrimes.

Tendências dos cibercrimes no Brasil:

Brasil já é considerado um polo do cibercrime mundial

Os custos do cibercrime são calculados com base nos valores referentes à perda de propriedade intelectual nas empresas, fraudes on-line e crimes financeiros

Jeferson Propheta, Administradores.com, 19 de março de 2018, às 12h49

Recentemente, a McAfee e a CSIS divulgaram um estudo informando que o cibercrime gera anualmente um prejuízo de quase US$ 600 bilhões para as empresas no mundo todo, um montante que representa cerca de 0,8% do PIB mundial. Na América Latina, a estimativa é de que as perdas com o cibercrime custem entre US$ 15 e 30 bilhões. Na realidade, esses números podem ser muito maiores, pois grande parte dos prejuízos causados por atacantes cibernéticos não são oficialmente registrados.

Os custos do cibercrime são calculados com base nos valores referentes à perda de propriedade intelectual nas empresas, fraudes on-line e crimes financeiros, custos de interrupção na produção ou serviços, custo de proteção de redes, recuperação após ataques cibernéticos, danos à reputação das marcas, entre outros prejuízos.

Uma novidade interessante reportada é que nos últimos anos o cibercrime no Brasil cresceu muito e o país passou a ser considerado um dos novos centros de cibercrime mundial, juntamente com a Índia, Coréia do Norte e Vietnã. O Brasil já é o alvo número um e a principal fonte de ataques na América Latina e, considerarmos o mundo todo, o país é a segunda principal fonte de ataques cibernéticos e o terceiro alvo mais afetado.

ONUBR Nações Unidas no Brasil

SOBRE A ONU | FAÇA PARTE | CAMPANHAS | ONU NO BRASIL | ESPECIAIS

INÍCIO | NOTÍCIAS DO BRASIL | AÇÃO HUMANITÁRIA | DESENVOLVIMENTO SUSTENTÁVEL | DIREITOS HUMANOS | PAZ E SEGURANÇA

Cibercrime movimenta US$1,5 trilhão por ano, diz ONU

Publicado em 05/07/2018 Atualizado em 05/07/2018

AUMENTAR LETRA DIMINUIR LETRA

Mais

O comitê da ONU com foco em prevenção ao crime e justiça criminal pediu uma resposta global mais integrada a desafios contínuos – incluindo o cibercrime. "Ainda há muito trabalho a ser feito", diz chefe da ONU sobre o tema.

Secretário-geral das Nações Unidas, Antônio Guterres, falando à imprensa na sede da ONU. Foto: ONU/Mark Garten

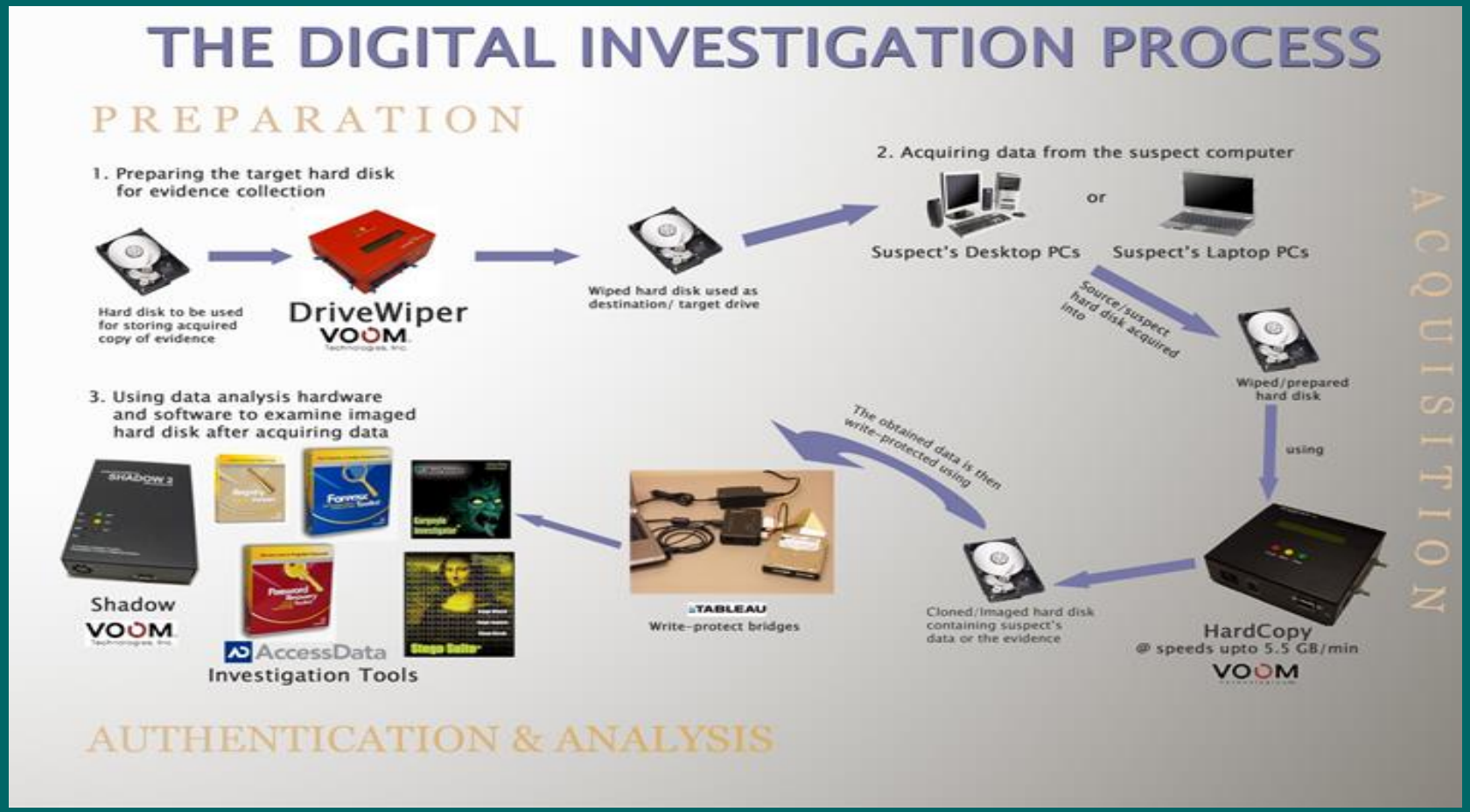
O comitê da ONU com foco em prevenção ao crime e justiça criminal realizou sua sessão anual em Viena pedindo uma resposta global mais integrada a desafios contínuos, entre eles o cibercrime.

Yury Fedotov, diretor-executivo do Escritório das Nações Unidas sobre Drogas e Crime (UNODC), reforçou a importância da cooperação para alcançar os Objetivos de Desenvolvimento Sustentável e combater a ameaça dos crimes virtuais.

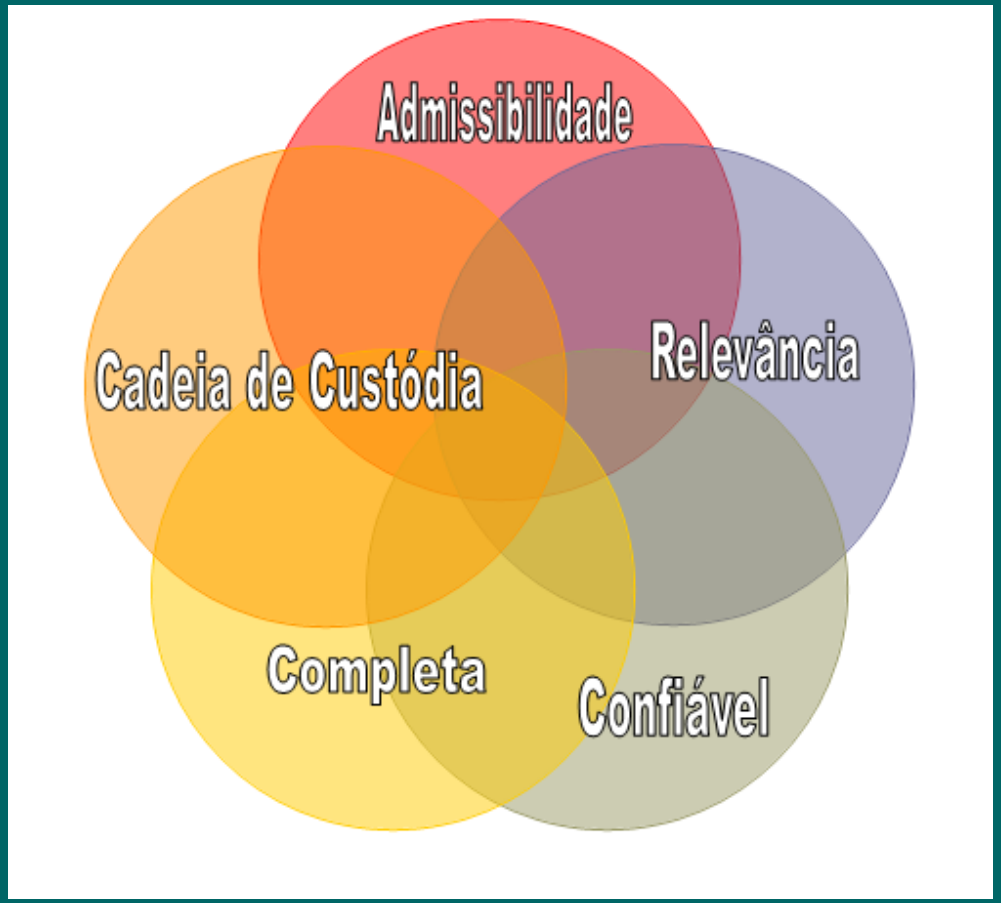
Problemas na investigação dos cibercrimes no Brasil:

1. Falta de harmonia entre a legislação penal brasileira e tratados internacionais sobre cibercrimes;
2. Falta de compartilhamento de dados entre órgãos policiais e empresas de serviços que atuam na internet, tanto dentro do país como fora dele;
3. Poucas unidades especializadas na investigação e prevenção de cibercrimes no país;
4. Falta de profissionais capacitados e experientes no combate aos cibercrimes nas unidades policiais brasileiras;
5. Inexistência de laboratórios bem aparelhados para suprir as necessidades periciais nas investigações de cibercrimes no país;
6. Emprego reiterado por órgãos policiais de buscas e apreensões apressadas (eficiencialismo exacerbado) por indícios de autoria ou por materialidade delitiva, ensejando a transgressão e a violação de direitos e garantias constitucionais como a privacidade e o devido processo legal.

Principais Etapas no Processo de Investigação de cibercrimes:



Requisitos para validade das provas eletrônicas:



Cenário Mundial para a Forense Computacional

- Alta dependência da Tecnologia da Informação;
- Virtualização da Sociedade (comunidades on-line, exemplo: Facebook, twitter, Orkut)
- Alta oferta de serviços on-line, desde instituições financeiras, até supermercados;
- Empresas tangendo e apoiando suas estratégias em componentes tecnológicos: significa fazer mais, melhor e com mais controle, em menor tempo e com menor custo.

A Identificação de evidências através da Forense Computacional

Diferentes crimes resultam em diferentes tipos de evidência, e, por este motivo, cada caso deve ser tratado de forma específica. Por exemplo, em um caso de acesso não autorizado, o perito deverá procurar por arquivos log, conexões e compartilhamentos suspeitos; já em casos de pornografia, buscará por imagens armazenadas no computador, histórico dos sites visitados recentemente, arquivos temporários e etc. A velocidade do perito em identificar as evidências vai depender do seu conhecimento sobre o tipo de crime que foi cometido e dos programas e Sistemas Operacionais envolvidos no caso.

A importância da adequada Análise de Evidências

As evidências digitais são delicadas por natureza, sendo necessário um profissional qualificado e que tenha conhecimento suficiente para realizar a análise forense de um sistema comprometido, ou que possua evidências necessárias para a comprovação de determinados fato.

Conclusão:

- Os meios eletrônicos, sobretudo a Internet, possibilitam a prática de crimes complexos, que exigem uma solução rápida e especializada. Podemos afirmar que os delitos virtuais crescem na proporção do avanço da tecnologia.
- Caso não ocorra uma rápida e intensiva especialização dos envolvidos na investigação e o uso de aparelhamento com tecnologia adequada, a batalha contra os cibercriminosos restará perdida.
- Cabe a iniciativa privada adotar providências para o combate a cibercriminalidade de forma supletiva a ação do Estado, inclusive quanto a capacitação de funcionários e troca de informações.

POLÍCIA CIVIL DE SÃO PAULO

“Cibercrimes: Uma Ameaça Atual e Efetiva”

JOSÉ MARIANO DE ARAUJO FILHO
Delegado de Polícia
josemariano@sp.gov.br

Acesse o nosso Blog:
http://www.delegadodepolicia.com

Twitter:
http://twitter.com/Digital_Crimes

Novembro/2018