A NOVA LEI 12.737/12

IMPLICAÇÕES NO TRATAMENTO DE INCIDENTES DE REDE

Serviço de Repressão a Crimes Cibernéticos
Coordenação Geral de Polícia Fazendária
Diretoria de Investigação e Combate ao Crime Organizado

INVASÃO DE DISPOSITIVO INFORMÁTICO

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Destaques:

- Invasão (conceito amplo; "força bruta" ou ardil)
- Dispositivo Informático (capacidade de processamento e/ou armazenagem)
- Mecanismo de Segurança (conceito amplo; sistema operacional)

PRODUÇÃO DE DISPOSITIVO OU SOFTWARE ILÍCITO

§1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

Destaques:

- *Phishing* (via de regra, ato preparatório)
- *Port Scan* (ato preparatório)

Obtenção de Informações Qualificadas e Controle Remoto

§ 3º Se da invasão resultar a OBTENÇÃO de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o CONTROLE REMOTO não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

- Obter Dados (significado amplo)
- Controle Remoto (BOTNETS)

Causas de Aumento de Pena

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

Ação Penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

INTERRUPÇÃO OU PERTURBAÇÃO DE SERVIÇO TELEGRÁFICO, TELEFÔNICO, INFORMÁTICO, TELEMÁTICO OU DE INFORMAÇÃO DE UTILIDADE PÚBLICA

Art. 266. Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento.
Pena - detenção, de um a três anos, e multa.

§ 1º Incorre na mesma pena quem INTERROMPE serviço telemático ou de informação de utilidade pública, ou IMPEDE ou DIFICULTA-LHE o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

- Utilidade Pública (abrangência)
- DDOS

Falsificação de Cartão de Crédito ou Débito

Falsificação de documento particular
Art. 298 Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
Pena - reclusão, de um a cinco anos, e multa.

Falsificação de cartão
Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (IN)

- Efeito prático

Minuta de Norma Complementar
Preservação de evidências e Comunicação à Polícia Federal

Serviço de Repressão a Crimes Cibernéticos
Coordenação Geral de Polícia Fazendária
Diretoria de Investigação e Combate ao Crime Organizado

HISTÓRICO

- Norma Complementar nº 08/IN01/DSIC/GSIPR:
  - 19 de agosto de 2010;
  - Objetivo: disciplinar o gerenciamento de Incidentes de Segurança em Redes de Computadores;
  - Realizado pelas ETIR;
  - Órgãos e entidades da Administração Pública Federal, direta e indireta - APF

NORMA COMPLEMENTAR Nº 08/IN01/DSIC/GSIPR

Capítulo 8 – Disposições gerais

8.5 Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais, as **ETIR têm como dever**, sem prejuízo do disposto no item 6 desta Norma Complementar e do item 10.6 da Norma Complementar nº 05/IN01/DSIC/GSIPR:

8.5.1 Acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários;

8.5.2 **Observar os procedimentos para preservação das evidências exigindo consulta às orientações sobre cadeia de custódia, conforme ato normativo específico a ser expedido**;

8.5.3 Priorizar a continuidade dos serviços da ETIR e da missão institucional da organização, **observando os procedimentos previstos no item 8.5.2**.

OBJETIVOS DA NOVA NORMA

- Estabelecer diretrizes para:
  - Registro de incidentes de segurança criminalizados;
  - Coleta e preservação dos registros e evidências;
  - Comunicação à autoridade policial competente.
- Interesse do Estado e da sociedade;
- Bens jurídicos tutelados penalmente (Lei nº 12.737/12, entre outras)

Das Ações Ilícitas

- Divulgação não autorizada de dado ou informação sigilosa, nos termos do art. 153, §1º-A do CP;
- Invasão de dispositivo informático, nos termos do art. 154-A do CP;
- Interrupção de serviço telemático ou de informação de utilidade pública, previsto no §1º do art. 266 do CP;
- Inserção ou facilitação de inserção de dados falsos, alteração ou exclusão de dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública, nos termos do art. 313-A do CP;

Das Ações Ilícitas

- Modificação ou alteração por funcionário público de sistema de informação ou programa de informática sem autorização, nos termos do art. 313-B do CP;

- Distribuição, armazenamento ou conduta vinculada a pornografia infantil, nos termos dos arts. 240, 241, 241-A, 241-B, 241-C e 241-D da Lei nº 8069/90;

- Interceptação telemática clandestina, nos termos do art. 10 da Lei nº 9296/96.

Das Ações Ilícitas

- Não se aplica aos atos preparatórios e às tentativas dos crimes listados

- A comunicação dos registros acima será objeto de ato normativo específico a ser expedido.

Coleta e preservação de registros

- A coleta e preservação dos vestígios deverão ser realizadas antes das ações de reestabelecimento do serviço afetado.
- Uso de mecanismos de sincronização de data, hora e fuso, como NTP.
- Atenção especial às mudanças de horário de verão.

EVENTOS E LOGS

- Eventos de autenticação, tanto os bem-sucedidos quanto os malsucedidos;
- Eventos de acesso e utilização de operações, recursos e dados privilegiados;
- Eventos de redução de níveis e/ou aplicação de filtros ao armazenamento de registros de auditoria (por exemplo, de *Warning* para *Error* ou *None*);
- Eventos de acesso a registros de auditoria;
- Outros eventos relevantes.

EVENTOS E LOGS

- Informações importantes:
  - Conta ou ID de usuário;
  - Tipo do evento (por exemplo, *logon*, *logoff* e tentativa de troca de senha)
  - Indicação de sucesso ou falha;
  - Data, hora e fuso horário;
  - Endereço IP, identificador de terminal, coordenadas geográficas, bem como toda e qualquer outra forma de identificação que possa ser registrada pelo ativo.

EVENTOS E LOGS

- Monitoramento e registro de eventos críticos:
  - Utilização de usuários, perfis e grupos privilegiados;
  - Inicialização, suspensão (tanto ordeira quanto forçada) e reinicialização de serviços/*daemons*;
  - Acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;
  - Modificações da lista de membros de grupos privilegiados;
  - Eventos obtidos de quaisquer mecanismos de segurança existentes, tais como *firewalls*, IDS/IPS, antivírus, SIEM, etc

OUTRAS ORIENTAÇÕES

- Se o ativo de informação permitir, uso de formato de log estendido (*extended log format*);
- Período mínimo de armazenamento: 06 meses;
- Se possível, uso de servidor remoto de armazenamento de registros de auditoria;
- Verificação periódica da implementação dos procedimentos descritos na Norma -> ETIR

NO CASO DE UM CRIME...

- Coleta das evidências:
  - Das mídias de armazenamento dos dispositivos afetados;
  - De todos os registros ou logs citados relativos ao crime, atos preparatórios e resultados produzidos.
- Quando for impossível preservar a mídia original, a ETIR deve realizar uma **cópia integral da mídia ou dos arquivos afetados** (cuidado com os metadados).

PRESERVAÇÃO DAS EVIDÊNCIAS

- Garantia de integridade:
  - Criar arquivo contendo os *hashes* de todos os arquivos coletados (algoritmo SHA256);
  - Gravar os arquivos coletados, juntamente com o arquivo de *hashes* citado;
  - Computar o *hash* SHA256 do arquivo de *hashes*.
  - Informar o *hash* anterior à autoridade policial competente.

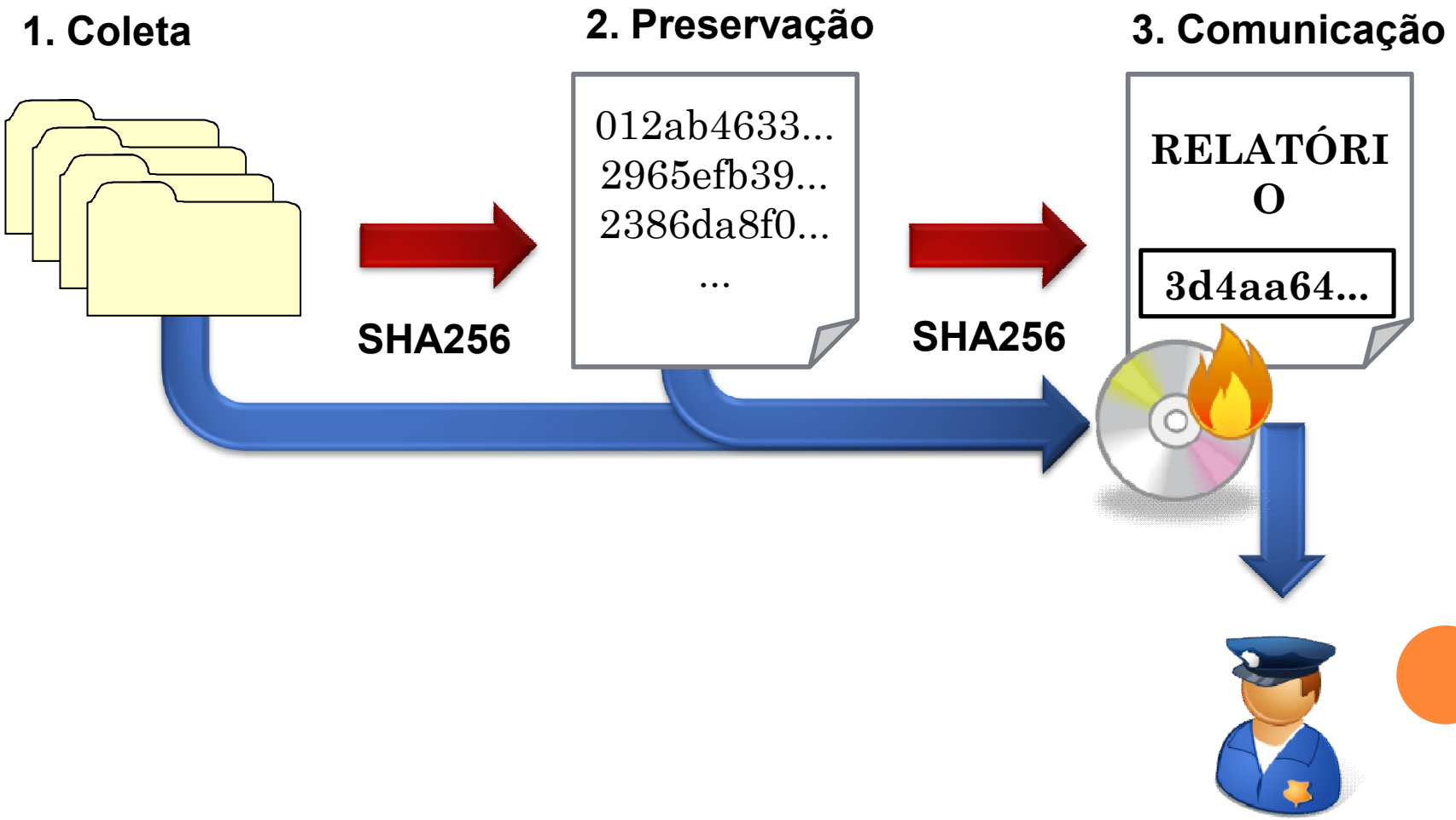
Comunicação à Autoridade Policial

- Após coletar as evidências, a ETIR deve comunicar a autoridade policial;
- Notícia-crime + relatório sobre o incidente;
- Destinatários:
  - Superintendência de Polícia Federal do estado onde se localiza o ativo;
  - Cópia ao Serviço de Repressão a Crimes Cibernéticos.

Relatório

- Nome, email e telefone do responsável pela preservação dos dados do incidente;
- Nome, email e telefone do responsável pela ETIR;
- Órgão comunicante e número da ocorrência;
- Relato circunstanciado sobre o incidente, descrevendo a natureza e origem dos dados coletados e preservados;
- Atividades de tratamento e outras providências tomadas pela ETIR, incluindo as ações de preservação, registrando como foi feito, ferramenta utilizada e local de armazenamento;
- *Hash* calculado do arquivo que contem a lista de hashes dos arquivos preservados.
- Outros (ver minuta).

Resumo dos Procedimentos



João Vianey Xavier Filho
Delegado de Polícia Federal
Serviço de Repressão a Crimes Cibernéticos
e-mail: *gpa.urcc@dpf.gov.br*

Flávio Silveira da Silva
Perito Criminal Federal
Serviço de Repressão a Crimes Cibernéticos
e-mail: *urcc.cgpfaz@dpf.gov.br*