Principais Aspectos da Segurança Cibernética relativos aos Órgãos da Administração Pública Federal nos Jogos Olímpicos e Paralímpicos RIO 2016

CTIR Gov

FOCO

ATIVOS DE INFORMAÇÃO

- **Pessoas**
- **Processos**
- **Ambiente**
- **Tecnologias**

ASSUNTOS

Ameaças

Protocolos de Notificação

CTIR Gov ⇄ **ETIR/APF**

Vídeo 1: https://www.youtube.com/watch?v=MK0SrxBC1xs

COMO AS AMEAÇAS SÃO VISTAS

Para os países desenvolvidos

- Espionagem
- Sabotagem
- Terrorismo
- Roubo

Para os países em desenvolvimento

- Fraudes bancárias
- Vazamento de dados

CENÁRIO ATUAL

Relatório da McAfee Labs revela novas ameaças de conluio entre aplicativos de dispositivos móveis

segs

Quinta, 23 Junho 2016 14:29 Fonte/Autor por: Medialink Comunicação Publicado em Info & Ti Imprimir E-mail Compartilhar::

G1

23/06/2016 20h49 - Atualizado em 24/06/2016 11h58

Hackers de Mogi movimentaram cerca de R$ 10 milhões, diz polícia

Air India: Police launch probe after hackers steal frequent-flyer miles worth Rs 1.6m

International Business Times

Brasil registra mais de 4 milhões de ciberataques

Risk Report 20/06/2016

20/06/2016 07:00 - Geral

Câmera de celular e até aparelhos de babá eletrônica são alvos de hacker

Para especialista, qualquer câmera num dispositivo com acesso à Internet é vulnerável

JCNET .com.br

TECNOLOGIA 20/06/2016 20:44

Coreia do Sul treina hackers em batalha contra o Norte

EXAME.COM

TENDÊNCIAS

- Aumento do número de oponentes.

TENDÊNCIAS

- Crescimento do CaS – *Cybercrime-as-a-Service*.

Cybercrime-as-a-Service

Cybercrime-as-a-Service

THE ORIGINAL HACKER FOR HIRE SERVICE - **THE #1 HACKER FOR HIRE** SERVICE IN THE WORLD

HiTech
CRIME SOLUTIONS

ENTERTAINERS - ATHLETES - POLITICIANS - CORPORATIONS - PARENTS - HUSBANDS/WIVES - CONSUMERS

HOME ABOUT US SPY SHOP BLOG

Hacking

- Have you been hacked?
- Do you want to find out if your website, computer or network can be or has been hacked?
- Would you like to hack into a computer, website or network?

Social Media Threats

- Has your Facebook, Twitter or Google+ account been hacked? We can help get it restored and track the person who did it in many cases.

Computer Spying and Surveillance

- Do you want to install spyware on a cellphone or computer?
- Do you want to know if you have spyware on your computer?

TENDÊNCIAS

- Aumento da sofisticação tecnológica dos oponentes, dificultando ainda mais a detecção e a reação.

Fonte: IAEA

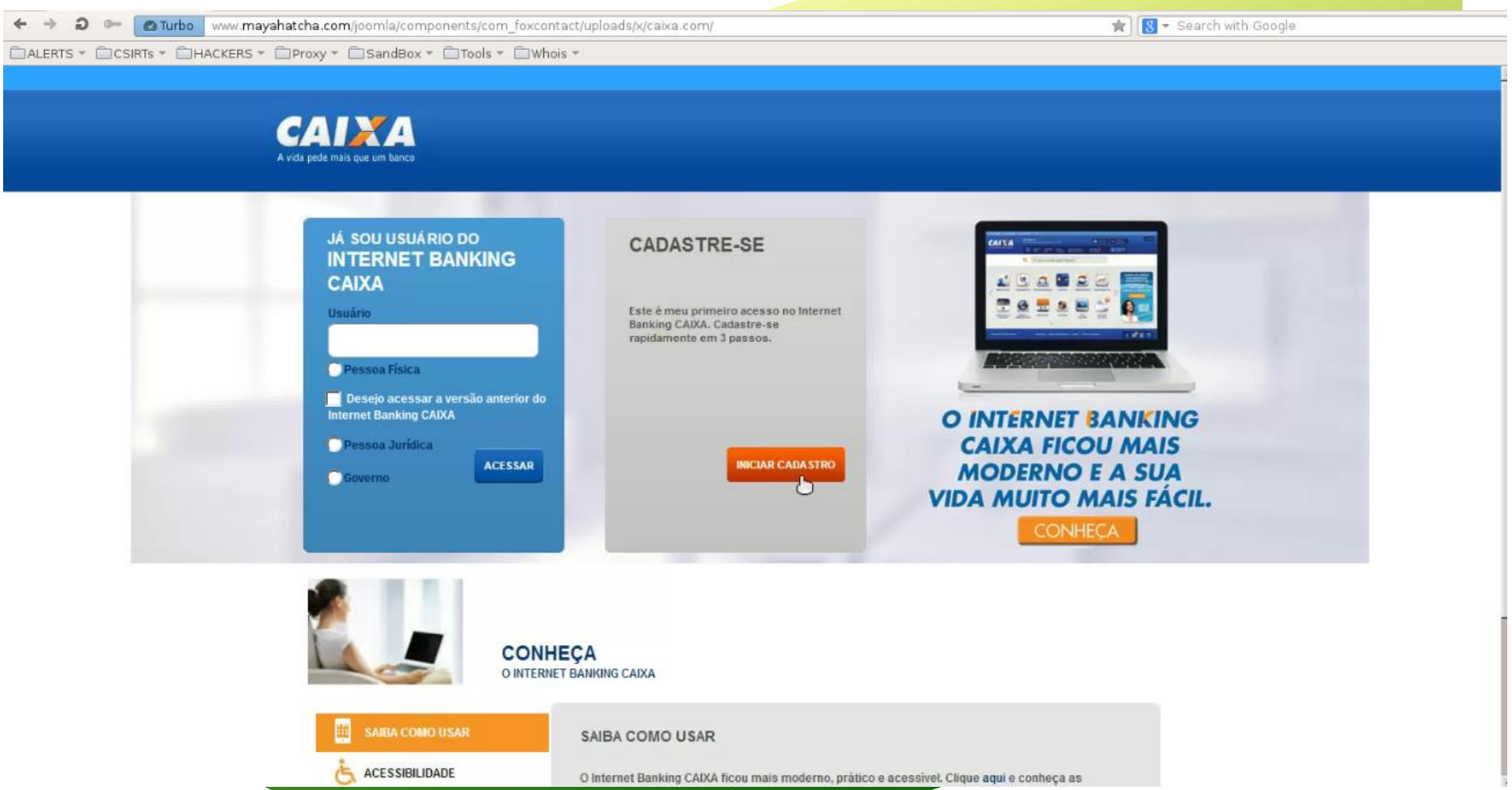
TENDÊNCIAS

- Crescimento dos *Spear Phishing* em detrimento das mensagens de *phishing*.

TENDÊNCIAS

- Crescimento dos sítios de *Phishing*.

Sítios de *Phishing*



TENDÊNCIAS

- Crescimento do **Ransomware**.

"Tipo de malware que restringe o acesso ao sistema infectado e cobra um valor de "resgate" para que o acesso possa ser reestabelecido."

Relatório de Pesquisa da Kaspersky Security Network:
718.536 pessoas foram afetadas por ataques de ransomware entre abril de 2015 e março de 2016.

Fonte: http://www.ibtimes.co.uk/crypto-ransomware-attacks-have-reached-epidemic-status-kaspersky-lab-says-1567366

RANSOMWARE

RANSOMWARE ATTACKERS REFUSE TO DECRYPT HOSPITAL'S FILES AFTER BEING PAID OFF

By **Justin Pot** — May 24, 2016

"Negotiating with criminals doesn't always work out, as Kansas Heart Hospital in Wichita learned last week. The hospital paid to get files back after falling victim to ransomware, but only got "partial access" and a demand for more money."

Fonte: http://www.digitaltrends.com/computing/ransomware-hospital-hackers-demand-more-money/

TENDÊNCIAS

- Incremento na capacidade dos oponentes de aliar ataques cibernéticos a consequências cinéticas.

Vídeo 2: https://www.youtube.com/watch?v=Oz3-NethUNY

TENDÊNCIAS

- Aumento das ameaças APT (*Advanced Persistent Threat*).
  - Pacientes e persistentes
  - Organizados
  - Custo elevado
  - Sofisticação: autoproteção, camuflagem, mutação
  - “O que for preciso!”
  - Organizações criminosas ou países

APT
Rússia *vs* Geórgia (2008)

- Geórgia *vs* Ossetas (apoiado pela Rússia).
- Negação de Serviço e Abuso de Sítios, conjugado com ataques por terra e ar.
- Sites governamentais, de empresas públicas e privadas foram tirados do ar.

APT
Stuxnet (2010)

- *Worm* de computador projetado especificamente para atacar o sistema operacional SCADA , desenvolvido pela Siemens para controlar as centrífugas de enriquecimento de urânio do Irã.
- Dupla função: fazer as centrífugas girarem 40% mais rápido por 15 min e inibir os sistemas de alarme.

APT
Sony (2014)

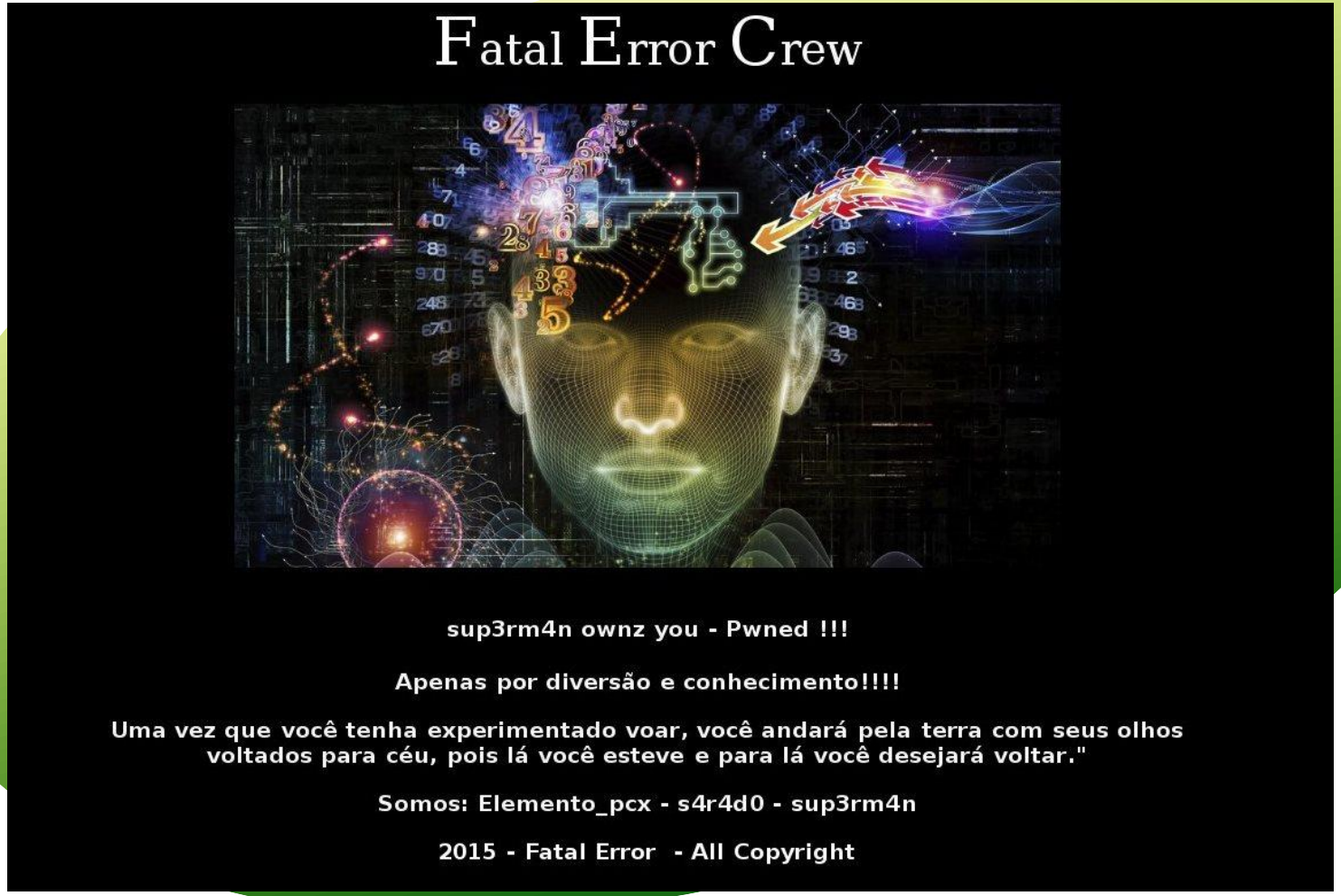
Guardians of Peace (GOP)

- Travou os PCs;
- Sobrescreveu os HD;
- Alterou os registros de boot;
- Bloqueou acesso a e-mails;
- Bloqueou acesso a rede interna.
- Prejuízo estimado: USD 100 milhões.

Fontes: http://thehackernews.com/2014/11/Sony-Pictures-Hacked.html
http://www1.folha.uol.com.br/tec/2014/12/1562817-entenda-o-caso-da-invasao-hacker-a-sony-pictures.shtml

TENDÊNCIAS

- Aumento do recurso de *defacement*.



Defacement


الجزائر مع فلسطين ظالمه او مظلومه
Algeria with Palestine unjust or oppressed

Defacement

|| HACKED ||

Su sistema tiene algunos fallos, fallos humanos por encima de los tecnicos.

El administrador no aprende de sus errores ni los corrige...

Una de mis intenciones es advertir los agujeros de seguridad presentes

Por estigmatizar la (in)seguridad es que estamos como estamos... Con nuestras instituciones vulnerables ante el mundo. ¿Es posible vivir en un mundo donde aprendamos de nuestros errores?

Anonymous_CCG - Colombian_Hackers

AMEAÇAS

Quais são nossas ameaças?

Vídeo 3: https://www.youtube.com/watch?v=-UjKf8SBDSo

Quais são nossas ameaças?

Funcionário não-confiável?

Extremistas?

Lobo solitário?

Grupos especializados?

Qual a origem das ameaças?

Internas	Externas
Infiltrado	Alvo de Oportunidade
Erro humano	Crime organizado
Insider	Lobo solitário
Infraestrutura	Extremistas
	Terroristas
	Estados-Nação

Ameaças Internas

Agente

Infiltrado

Sabotador

Ameaças Internas

Erro humano

Procedimentos

Conhecimentos

Violações

Projetos de Segurança

Ameaças Internas

Ameaças Internas

Insider

- Funcionário desapontado
- Acesso às redes
- Cooptado por organização terrorista
- Roubo, espionagem, sabotagem, dano
- Desentendimentos no processo de demissão
- Nível de privilégio de acesso
- Cooptado por organização criminosa

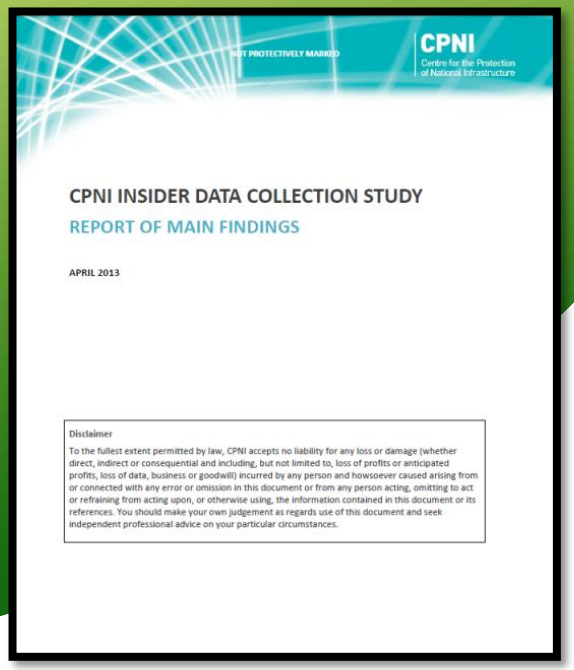
Vídeo 4: https://www.youtube.com/watch?v=HtTUsOKjWyQ

Vídeo 5: https://www.youtube.com/watch?v=-bkxOo41VSg

Ameaças Internas

Quem é o Insider?

- Frequentemente objeto de *bullying*.
- Versado em computação – conhecimento de grupos hacker; acesso remoto; planeja os ataques.
- Graves problemas de relacionamento familiar.
- Problemas financeiros.
- Notoriamente insatisfeito.
- Desejo de reconhecimento.
- Lealdade a amigos, parentes, etc.
- Vingança



Fonte: Insider Threat Study – 2013, CPNI Report

Ameaças Internas

Vazamento não intencional

- Enviar documento por email
- Copiar e colar
- Publicar sem autorização
- Renomear documento
- Alterar o tipo de documento
- Copiar dados parcialmente
- Apagar senhas

Vazamento malicioso

- “Printar” a tela
- Codificar caracteres
- Ocultar os dados
- Fotografar os dados

Fonte: IAEA

Ameaças Internas

Segundo o "Insider Threat Study – 2013", os *insiders* descobertos haviam incorrido nas seguintes ações:

- Divulgação não autorizada de informações sensíveis.
- Processos de corrupção.
- Facilitação de acesso a terceiros aos ativos de informação da organização.
- Sabotagem física.
- Sabotagem de TI.

Fonte: Insider Threat Study – 2013, CPNI Report

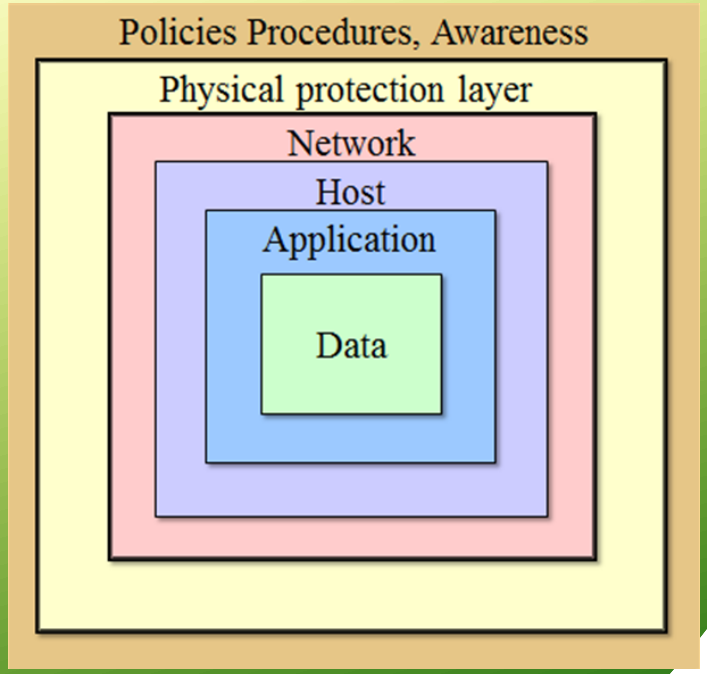
Ciclo de Vida do Empregado

Contratação | Desempenho | Transferência | Término

Vídeo 6: https://www.youtube.com/watch?v=PMZ24C9DCZA

Controles de Acesso

- Defesa em profundidade
- Algo que você sabe
- Algo que você possui
- Algo que você é



Instalações de tratamento de esgoto do Condado de Maroochy, Queensland, Australia (2000)

- Vitek Boden trabalhava na Hunter Watertech (instalou o sistema de tratamento de Maroochy)
- Em 1999 foi demitido (mas permaneceu por um tempo).
- Tentou emprego no Conselho do Condado mas foi recusado.
- Plano: vingar-se de ambos, lançando ataques contra o sistema SCADA para que a empresa fosse culpada.

Fonte: http://pt.slideshare.net/somnerville-videos/maroochy-water-breach

Instalações de tratamento de esgoto do Condado de Maroochy, Queensland, Australia (2000)

- Possuía um programa de configuração do SCADA que instalou em seu notebook.
- Possuía um rádio e um computador da empresa que podia simular um computador de controle de uma estação de bombeamento.
- Mudou as configurações dos controles das estações de bombeamento.

Mais de 1 milhão de litros de esgoto não tratados foram lançados em vias fluviais e parques públicos.

Vídeo 7: https://www.youtube.com/watch?v=fJyWngDco3g

Fonte: http://pt.slideshare.net/somnerville-videos/maroochy-water-breach

Ameaças Internas

Infraestrutura

- Atenção à integração das redes de segurança.
- Mecanismos de segurança física.

Hackers usam milhares de câmeras de segurança "zumbis" para atacar site

OLHAR DIGITAL SEGURANÇA

REDAÇÃO OLHAR DIGITAL 28/06/2016 10H06

Ameaças Externas

Identificado em varredura

Alvo de Oportunidade

Alvo compensador

Ameaças Externas

- Crime Organizado
- Negócios ilícitos
- Suporte financeiro
- Extratificação de funções

MAIS DE UM MILHÃO DE IPS FORAM UTILIZADOS EM TENTATIVA DE INVASÃO A EMPRESAS

Hackers hit central banks in Indonesia and South Korea

Fonte: DPF

Ameaças Externas

Lobo solitário

- Causar danos
- Motivação religiosa
- Motivação ideológica
- Apoio pessoal a uma causa

Fonte: http://motherboard.vice.com/read/what-is-a-lone-wolf-terrorist

Ameaças Externas

Extremistas

- **Propagar mensagem**
- **Motivação ideológica**
- **Apoio a uma causa**

Ameaças Externas

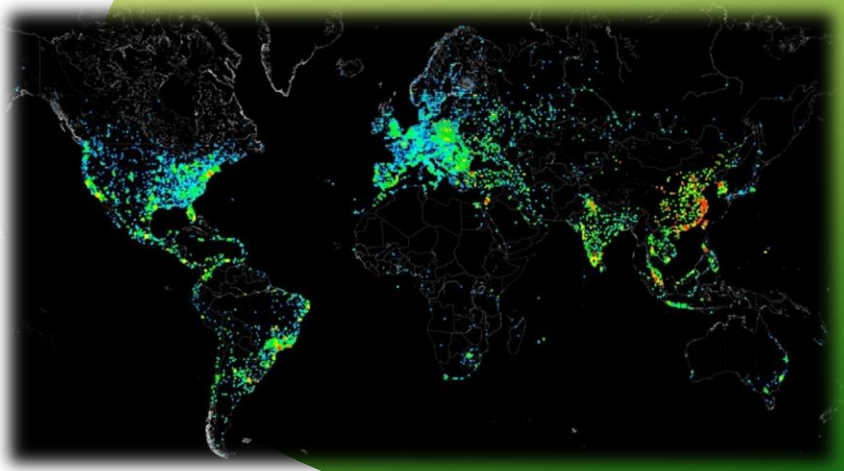
Terroristas

- Mensagem de ódio
- Maior dano possível
- Motivação religiosa
- Boa organização

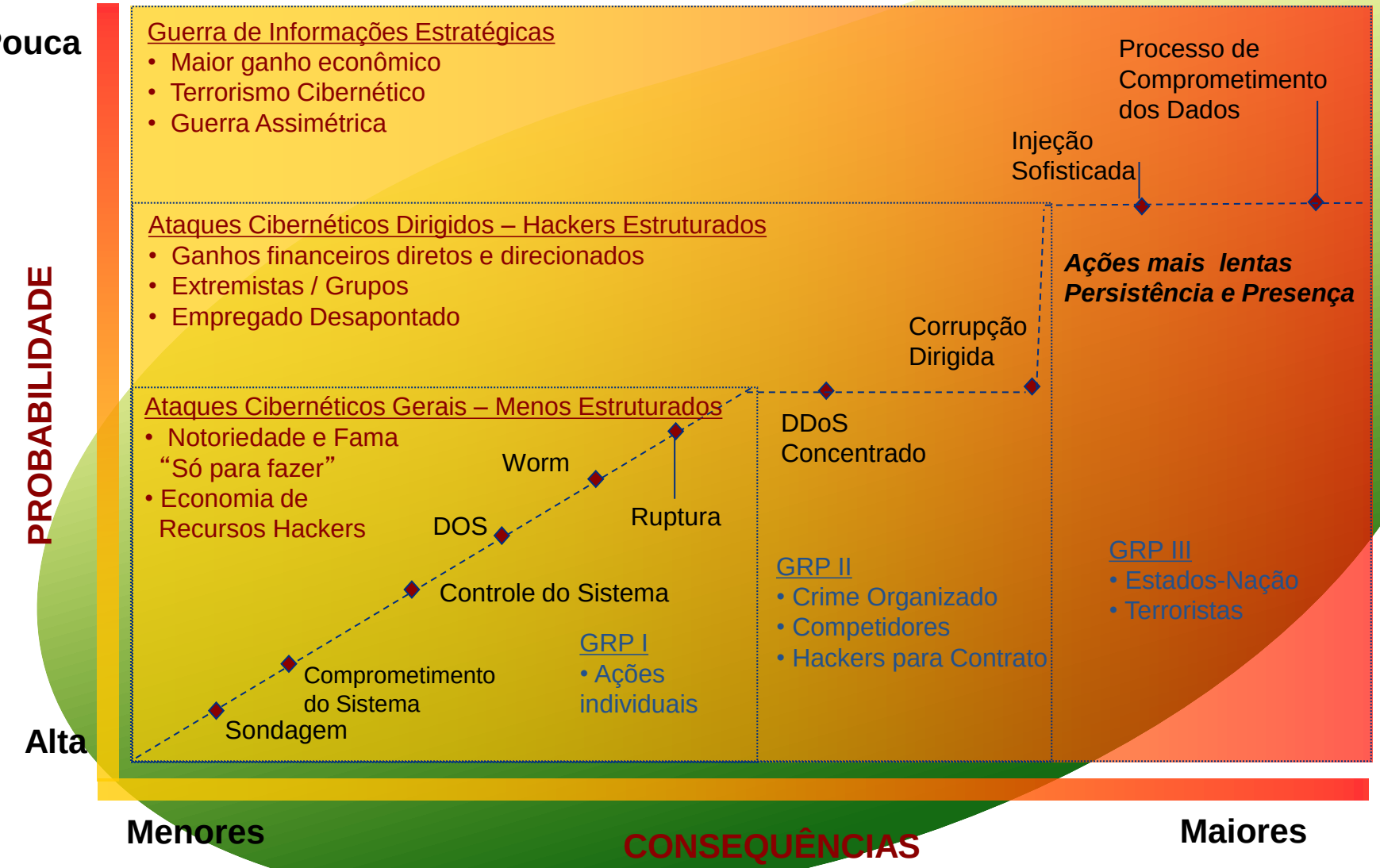
Ameaças Externas

Estados-Nação

- **Muitos recursos**
- **Muito boa organização**
- **Segredos industriais**
- **Infraestruturas Críticas**



Características das Ameaças



Fonte: IAEA

Aspectos que favorecem o Atacante

Habilidade

Capacidade

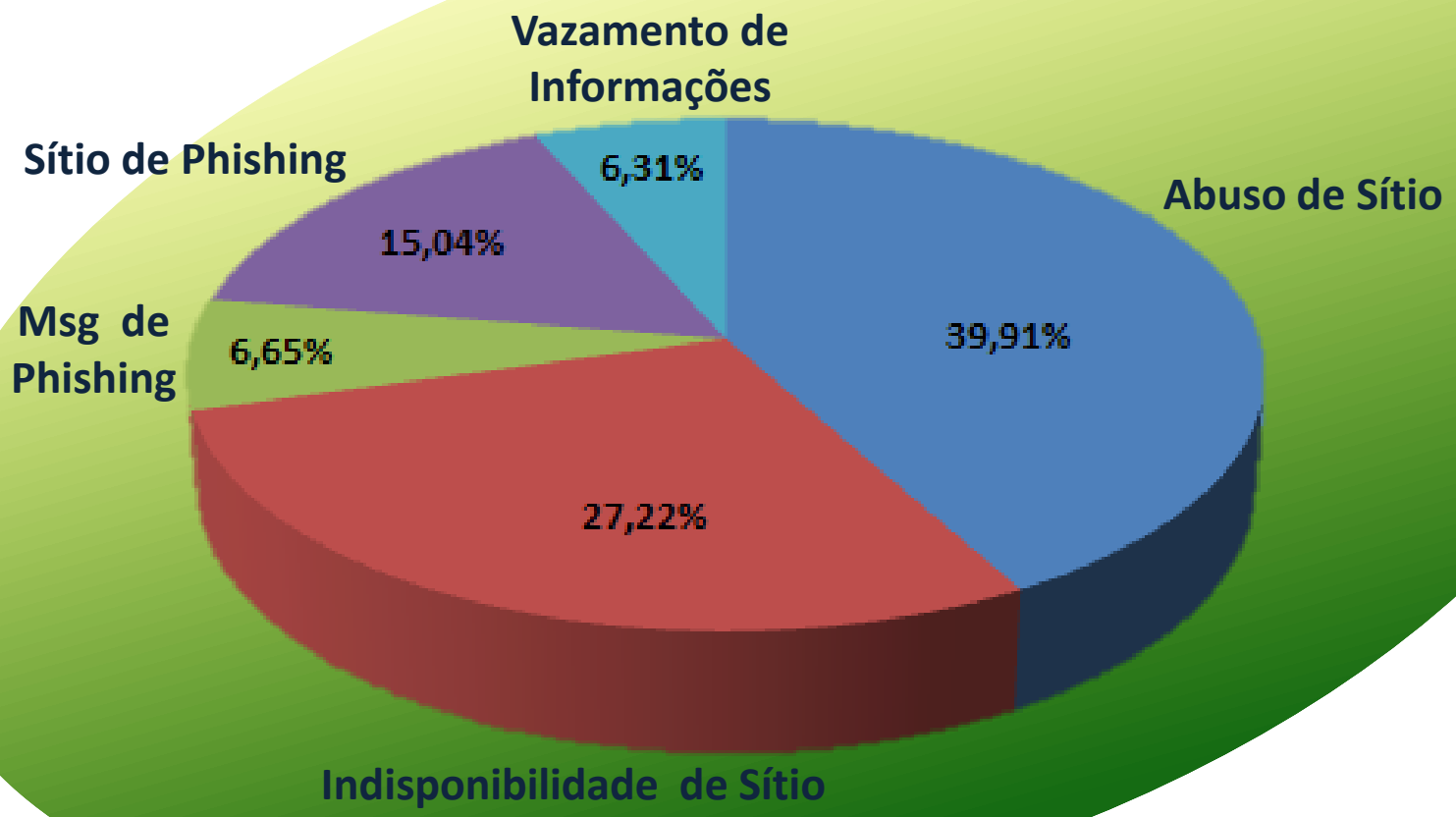
Oportunidade

Motivação

Vídeo 8: https://www.youtube.com/watch?v=32JgSJYpL8o

Vídeo 9: https://www.youtube.com/watch?v=zcmmFQGxMNU

Principais Incidentes – APF (Jan a Jul/16)



Principais Tipos de Ataques em Grandes Eventos

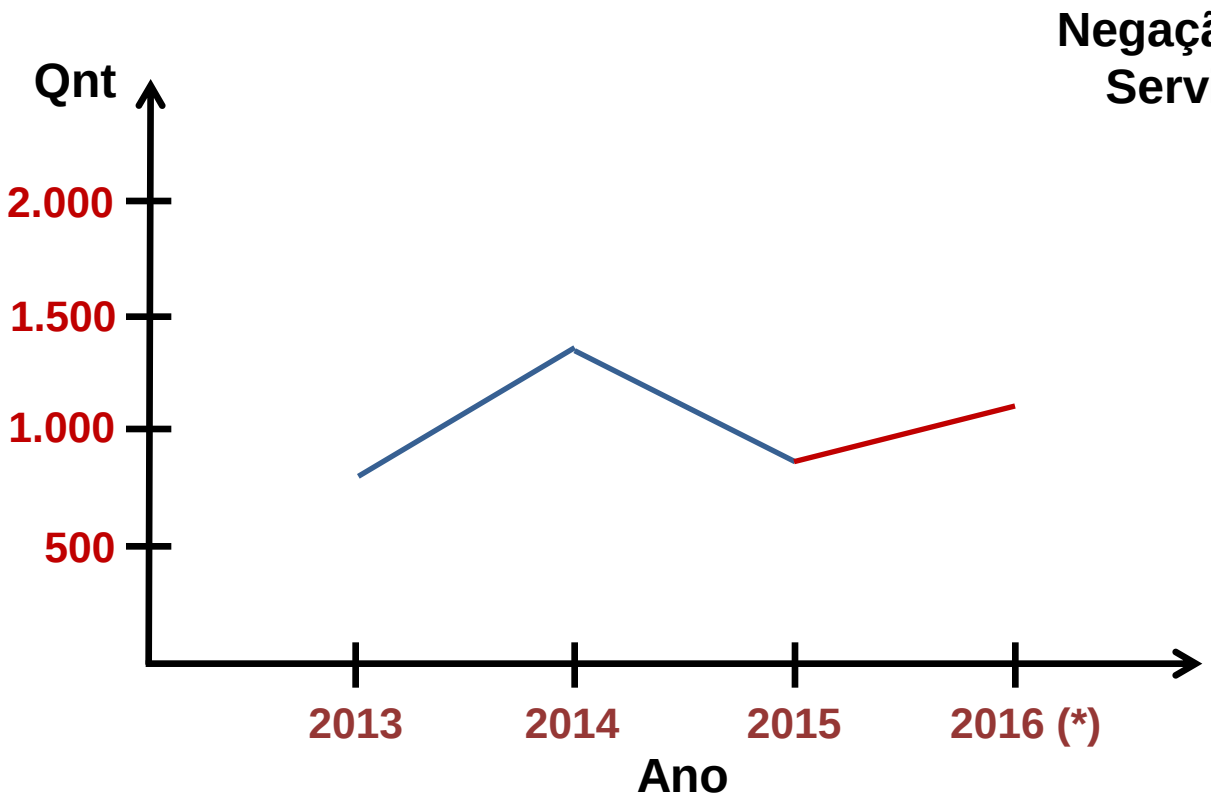
Negação de Serviço (DDoS)

Abuso de Sítio

Engenharia Social

Exposição de Info Sensíveis

Negação de Serviço (*Distributed Denial of Service* - DDoS)



Negação de Serviço (*Distributed Denial of Service* - DDoS)

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

"Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS)"

http://www.cert.br/docs/

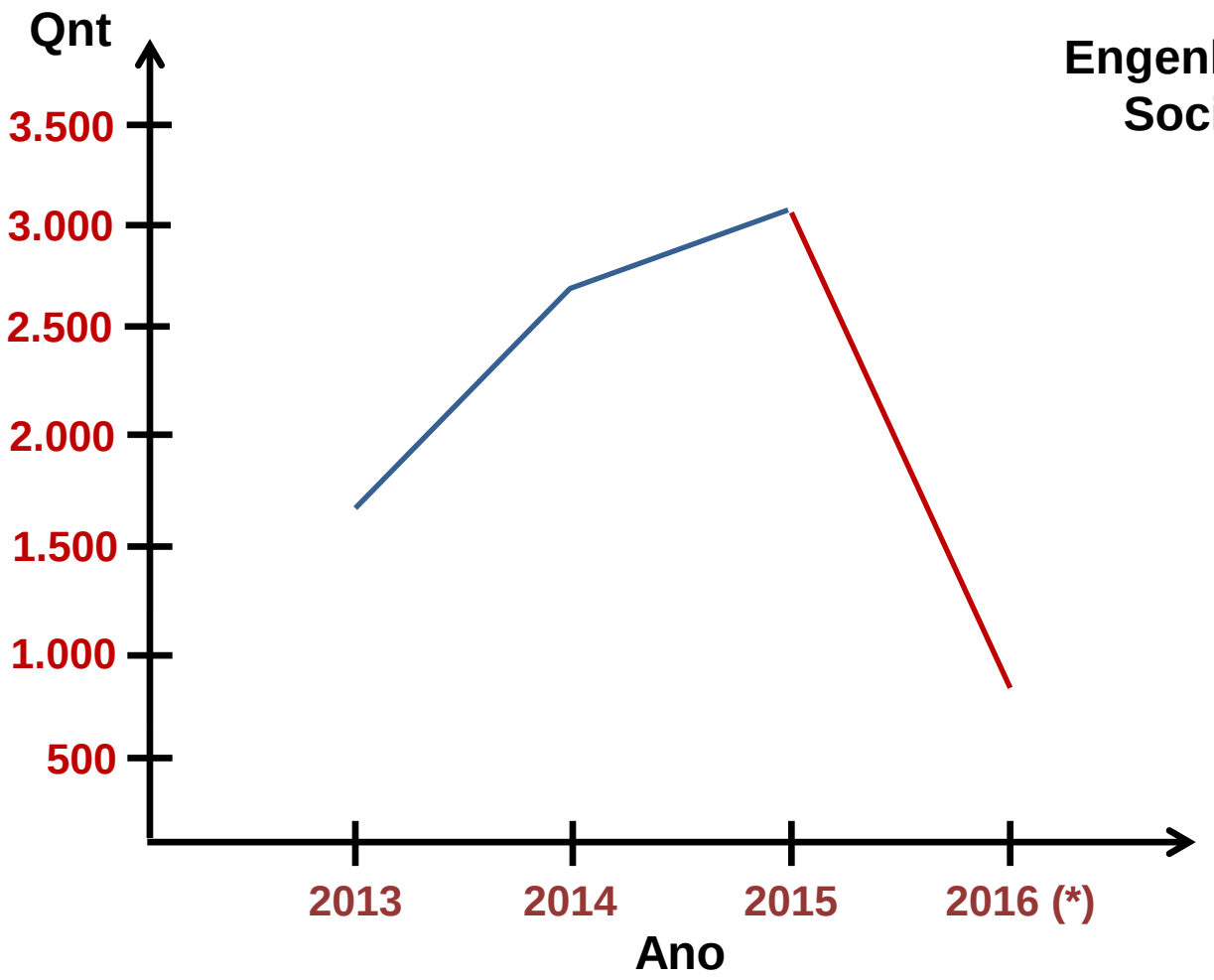
Engenharia Social

Pessoas

Ativo mais crítico das organizações

Capacitação, Treinamento, Sensibilização

Engenharia Social



Exposição de Informações Sensíveis

- Grupo de hackers: *Impact Team*.
- Protesto à não exclusão total dos dados dos usuários que solicitavam a remoção dos seus dados.
- Exposição dos dados de mais de 37 milhões de usuários.
- Alvo de investigação na Comissão Federal de Comércio (FTC).

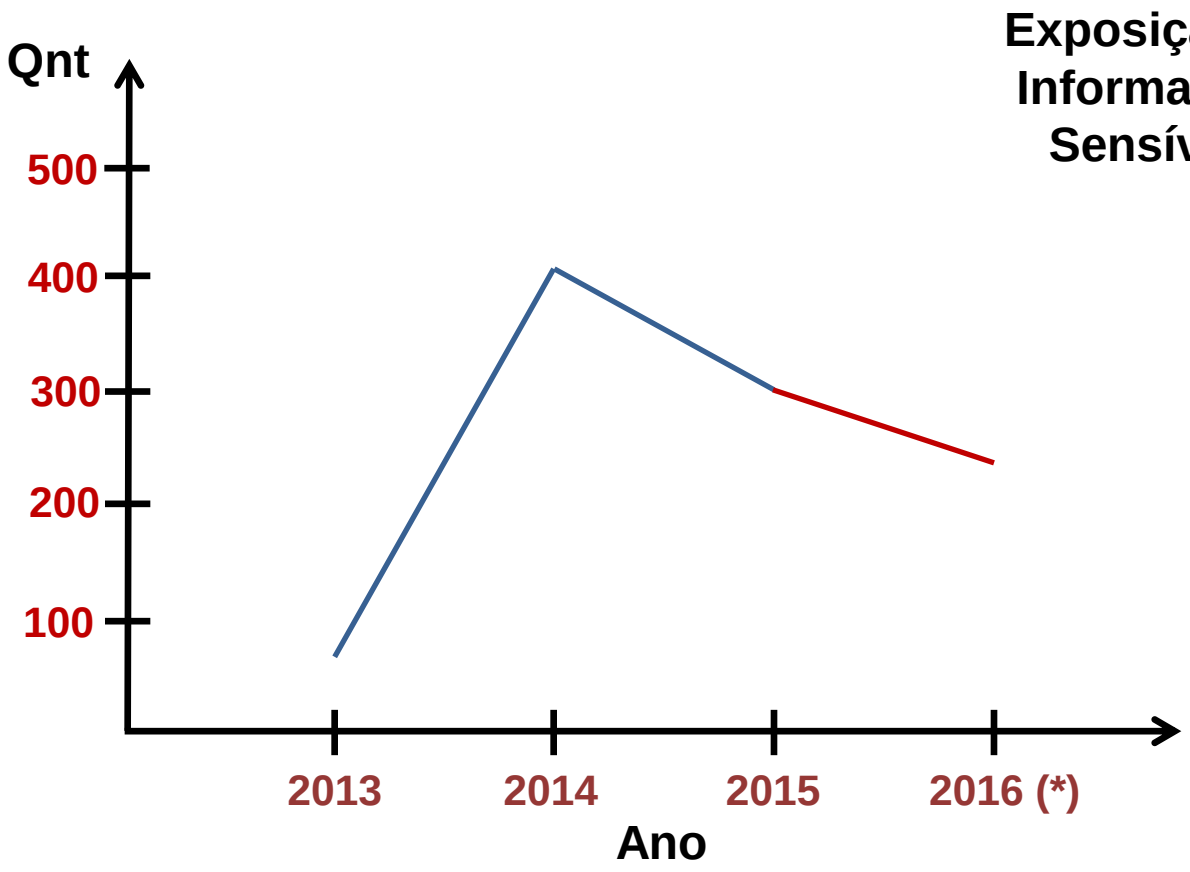
Fonte: http://g1.globo.com/tecnologia/noticia/2016/07/site-de-traicao-ashley-madison-e-alvo-de-investigacao-nos-eua.html

Exposição de Informações Sensíveis

- Aquisição / teste de software: preocupação com exfiltração de dados, atualizações e repositórios.

Vídeo 10: https://www.youtube.com/watch?v=HuJJFKmRYS0

Exposição de Informações Sensíveis



Abuso de Sítio

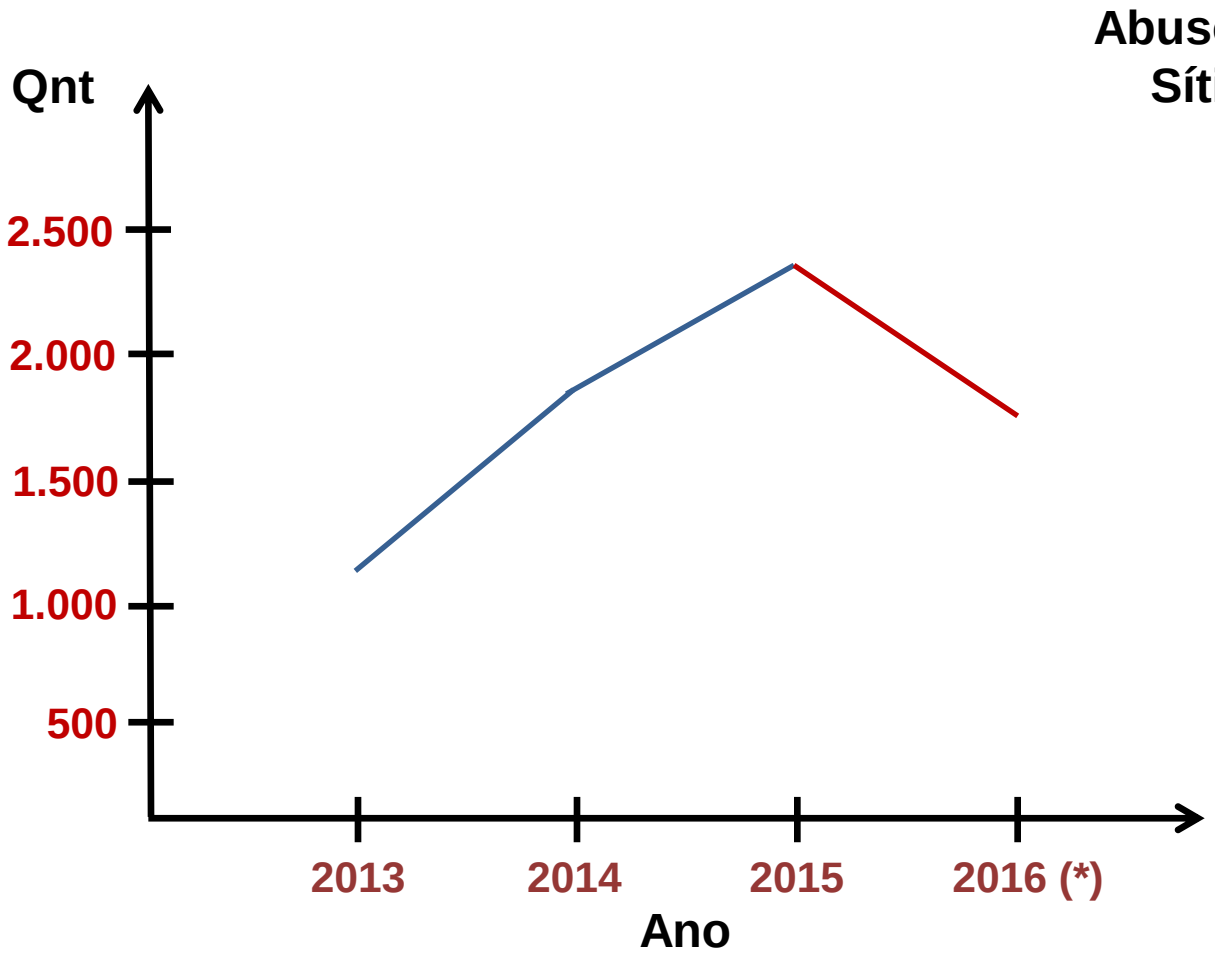
Hacked By Anarchy Ghost

Hackeado por Sm0ld3r

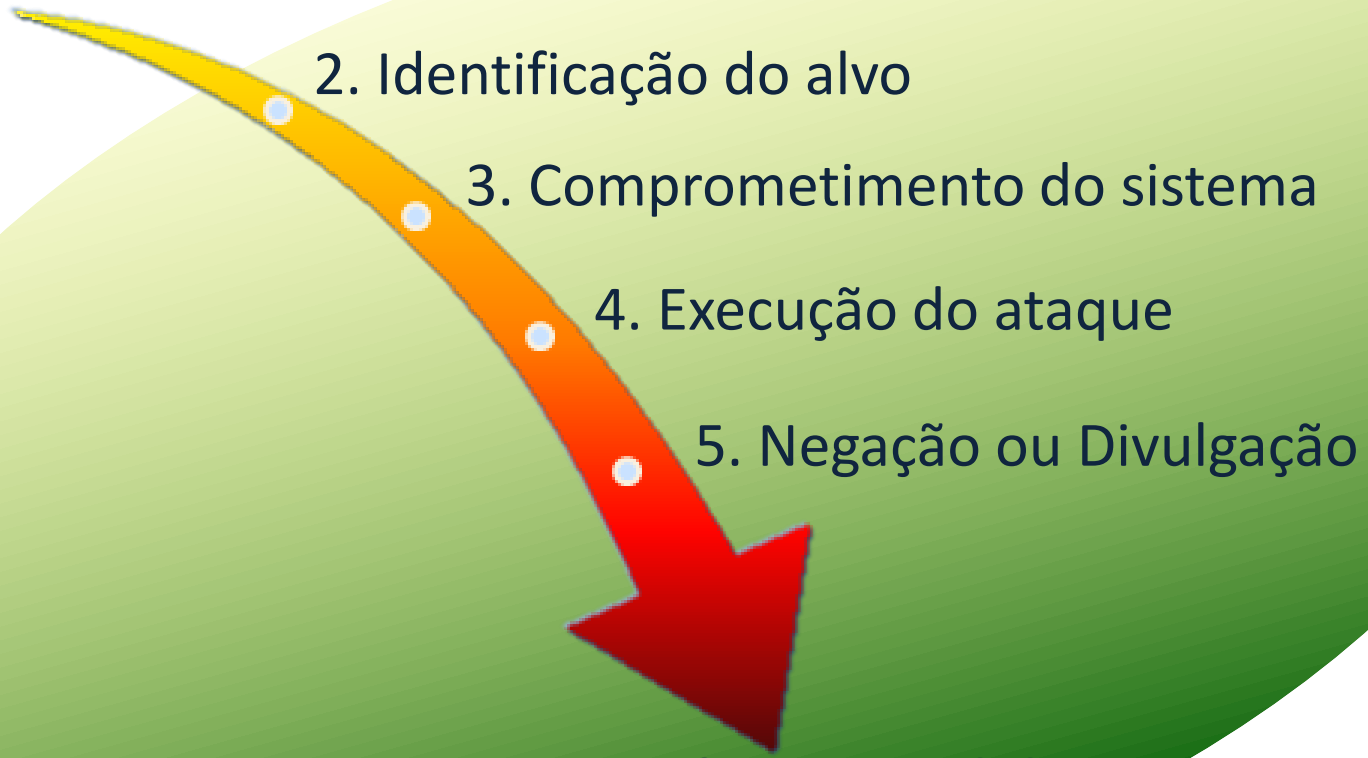
Hoje é dia de cobrança e quem deve vai morrer !!

Abuso de Sítio

Principais Tipos de Ataque em Grandes Eventos



Sequência de um Ataque



Fonte: IAEA

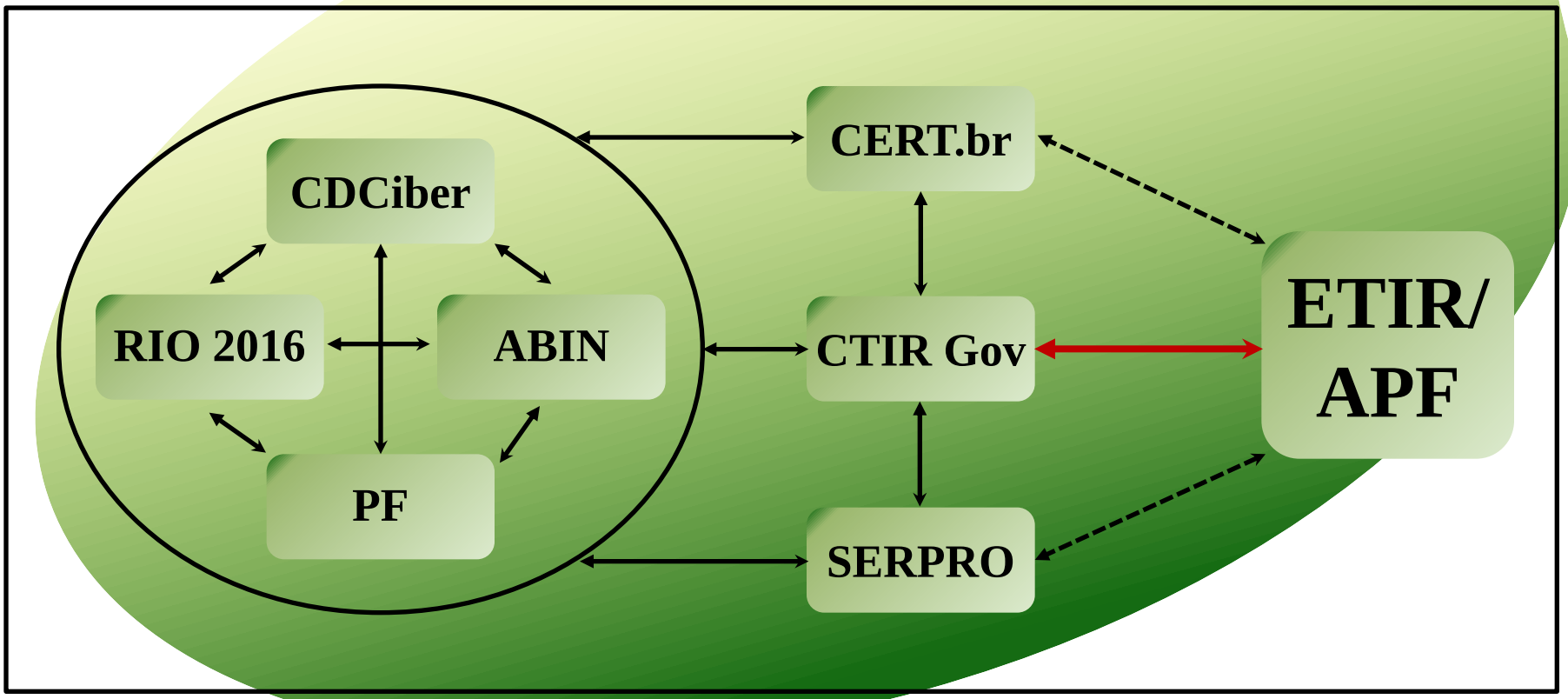
Protocolo de Notificações

Princípios

Simplicidade
Objetividade
Clareza
Celeridade
Economia de meios

Protocolo de Notificações

Ligações



Protocolo de Notificações

Procedimentos

Dias Úteis
(08:00 às 19:00 hs)

Dias não úteis e dias úteis
(após às 19:00 hs)

Dias Úteis (08:00 às 19:00 hs)

- A notificação deverá ocorrer pelo e-mail ctir@ctir.gov.br
  - Diferença entre “Para” e “CC”.
  - Inserir a Tag [RIO2016] no campo “Assuntos” nas mensagens que tenham relação com a segurança do evento.

- Caso o órgão deseje realizar maiores esclarecimentos:
  - Telefone INOC (10954*810); ou
  - Telefone de sobreaviso (61-99995-7859).

- Contato do CTIR Gov com os órgãos: **e-mail** e **Telefone.**

Dias não Úteis/dias Úteis (após às 19:00 hs)

- A notificação deverá ocorrer pelo e-mail ctir@ctir.gov.br
- O CTIR Gov também deverá ser contatado pelo telefone de sobreaviso (61-99995-7859).
- Contato do CTIR Gov com os órgãos: **e-mail e telefone.**

Contatos

E-mail: ctir@ctir.gov.br

INOC-DBA BR: 10954*810

Sobreaviso (24 hs): 61-99995-7859

Chave PGP (pública):
http://www.ctir.gov.br/arquivos/certificados/ctir2009.asc

CONSIDERAÇÕES FINAIS

- Crença no trabalho realizado.
- Respeito às características de todos os órgãos.
- Intensa disseminação de informações.
- Respeito aos ativos de informação dos órgãos.
- Reforço à mentalidade preventiva.
- Incentivo ao multi-preparo.
- Relevância ao uso de indicadores.
- Busca da resiliência.
- Cooperação, integração e confiança.


Fizemos Ontem,
Fazemos Hoje,
Faremos Sempre!

Muito Obrigado!

arthur.sabbat@presidencia.gov.br

(61) 3411-4383