

Incorporar Segurança Digital nas organizações é uma questão **fundamental**



Italo Valcy <italovalcy@ufba.br>

01/Out/2018, IX WTR do PoP-BA

Muitas notícias de ataques, fraudes, problemas de segurança digital...

POR O GLOBO

14/03/2018 11:00 / atualizado 14/03/2018 13:33



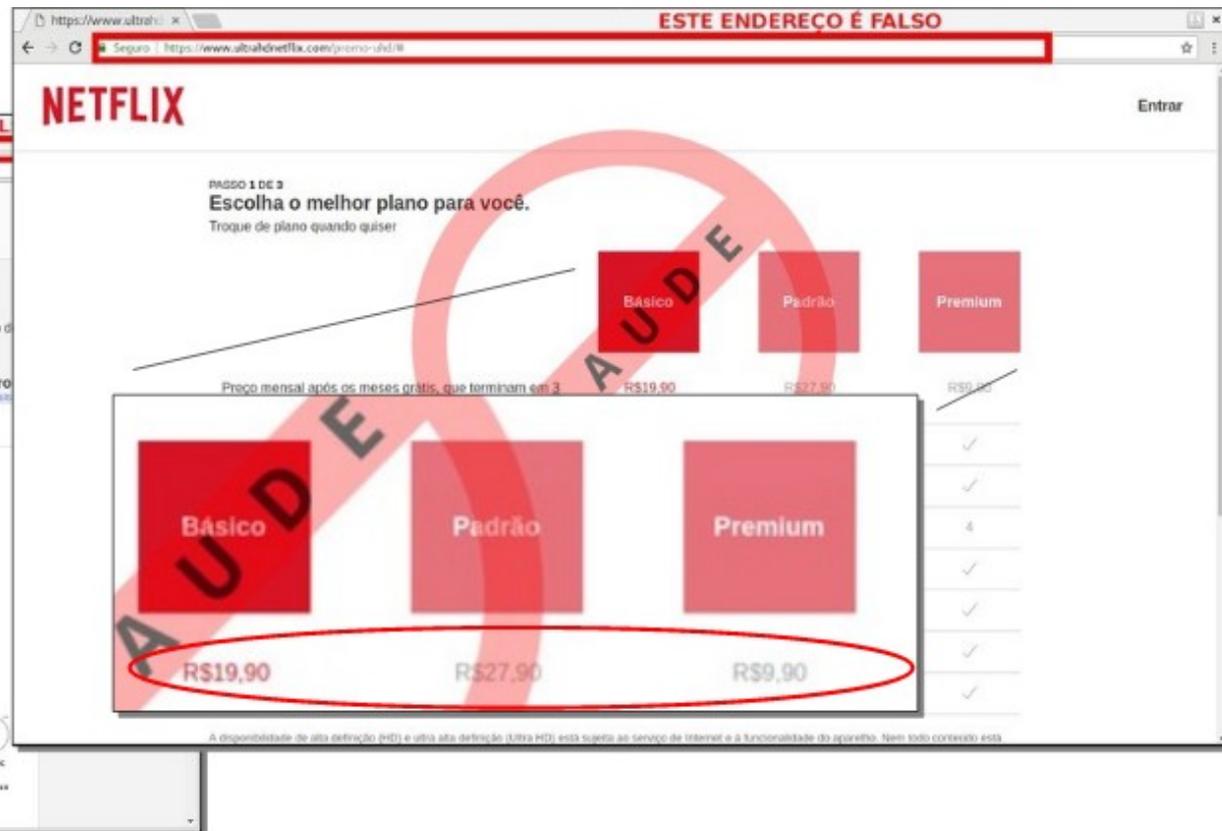
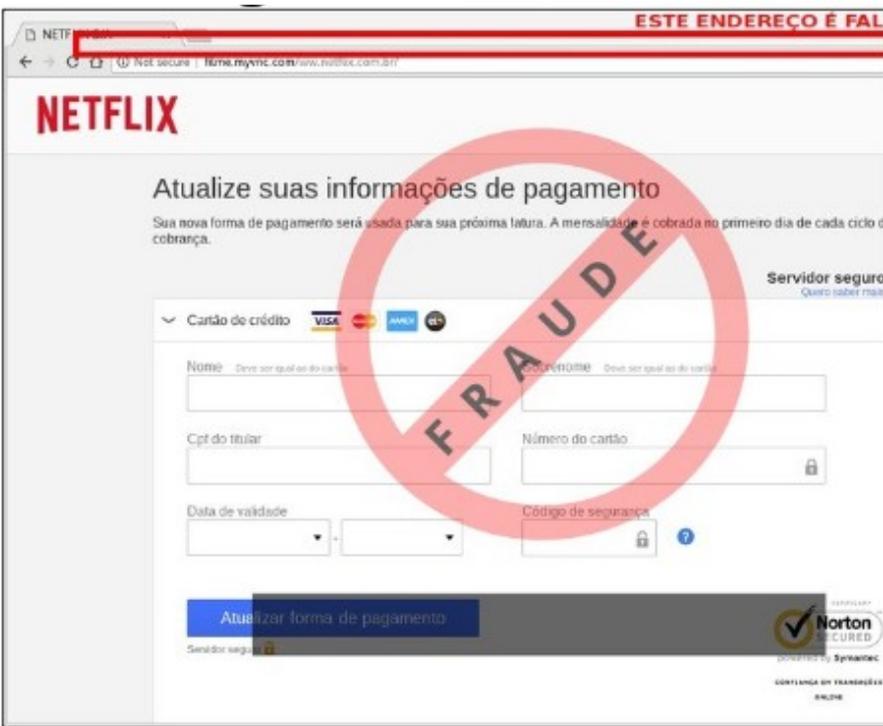
RIO — Um, dois, três, quatro... golpe. A cada cinco segundos, alguma empresa de comércio eletrônico brasileiro sofre algum tipo de fraude. É o que indica um estudo da Konduto, empresa especializada em segurança-online. Só no setor bancário houve um aumento de quase 300% das queixas referentes à quebra de sigilo e à segurança dos canais de acesso às contas pela web, segundo dados do Banco Central.

<https://oglobo.globo.com/economia/defesa-do-consumidor/golpes-na-internet-veja-as-fraudes-mais-comuns-como-se-proteger-22485183>

Phishing ainda é um dos principais vetores



Como identificar e se prevenir?



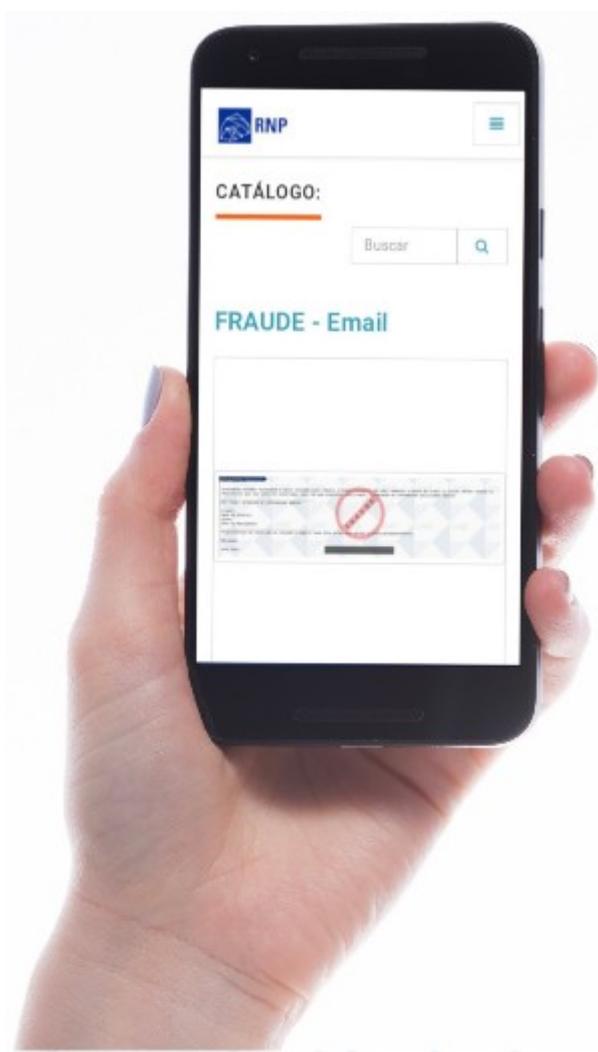
Como identificar e se prevenir?

- Catálogo de Fraudes da RNP: nova versão
- Um novo conceito para o mapeamento de fraudes na rede acadêmica brasileira
- Reportar fraudes:
 - phishing@cais.rnp.br

Acesse: catalogodefraudes.rnp.br

Como identificar e se prevenir?

- Catálogo de Fraudes da RNP: nova versão



Entretanto, e as fraudes mais elaboradas?

- Conhecimento dos processos internos da organização
 - Atacantes fazem seu home work
- Gramaticalmente, o e-mail pode ser perfeito
- A página fraudulenta pode ser idêntica à original, o link pode ser até o mesmo!
- Nem sempre você precisa clicar ou fazer o download
- As vezes somos vítimas apenas por acessar o site
 - XSS, CSRF, CoinHive

Entretanto, e as fraudes mais elaboradas?

Início ▾ Bitcoin ▾ Nova fraude envolvendo Bitcoin diz que vai expor seus hábitos de assistir...

Nova fraude envolvendo Bitcoin diz que vai expor seus hábitos de assistir vídeos adultos

Hackers estão alegando ter filmado tudo o que você assistiu online - é uma farsa

Por Mateus Nunes - 16/07/2018 07:30 37

Fonte: <https://livecoins.com.br/nova-fraude-envolvendo-bitcoin-diz-que-vai-expor-seus-habitos-de-assistir-videos-adultos/>

Entretanto, e as fraudes mais elaboradas?

CONVITE - Mozilla Thunderbird

Arquivo Editar Ver (X) Ir Mensagem Enigmail Ferramentas Ajuda

Receber mensagens Nova msg Bate-papo Catálogo Tags

Responder Re: Todos Encaminhar Mais

De [Redacted] <[Redacted]@gmail.com>

Assunto CONVITE 20-06-2018 09:56

Para undisclosed-recipients;

Cco: [Redacted].br

Caro Colegas, Estudantes e Amigos, bom dia !

Conforme indicação do [Redacted] FILHO; solicito a gentileza de verificar com urgência a disponibilidade de poder participar ou indicar alguém de confiança para integrar o quadro funcional das vagas disponíveis para coordenadores e auxiliares para prestação de serviços temporários em Processos Seletivos. (obs: vale ressaltar que esse trabalho não terá vínculo nenhum empregatício e pode ser profissionais de qualquer área e qualquer Instituição de Ensino).

Tenho um amigo que é dirigente de uma Comissão de Vestibulares & Concursos de algumas Universidades Particulares, Estaduais e Federais no Brasil que procura alguns profissionais que tivessem condições de exercer estas funções informadas abaixo e serem contratados imediatamente para prestar serviços em Vestibulares e Concursos. OBS:NÃO É SELEÇÃO; AS PESSOAS INDICADAS SERÃO CONTRATADAS IMEDIATAMENTE.

VAGAS

- * 08 vagas p/ Vice Coordenadores
- * 08 vagas p/ Coordenadores
- * 08 vagas p/Supervisores de Departamento
- * 08 vagas p/ Auxiliares de Aplicação
- * 08 vagas p/Auxiliares de Coordenação
- * 08 vagas p/Auxiliares de Aplicação
- * 08 vagas p/Auxiliares de Corredor

CARGA HORÁRIA
Horário de Trabalho - das 07 às 14h

REMUNERAÇÃO

- *R\$225,00 - Auxiliar de Corredor - por dia - 1º grau completo
- *R\$295,00 - Aux. Aplicação - por dia - 2º grau completo
- *R\$420,00 - Aux. Coord. por dia - universitário ou nível superior qualquer área
- *R\$750,00 - Vice Coord. por dia - Pós Graduando Lato Sensu

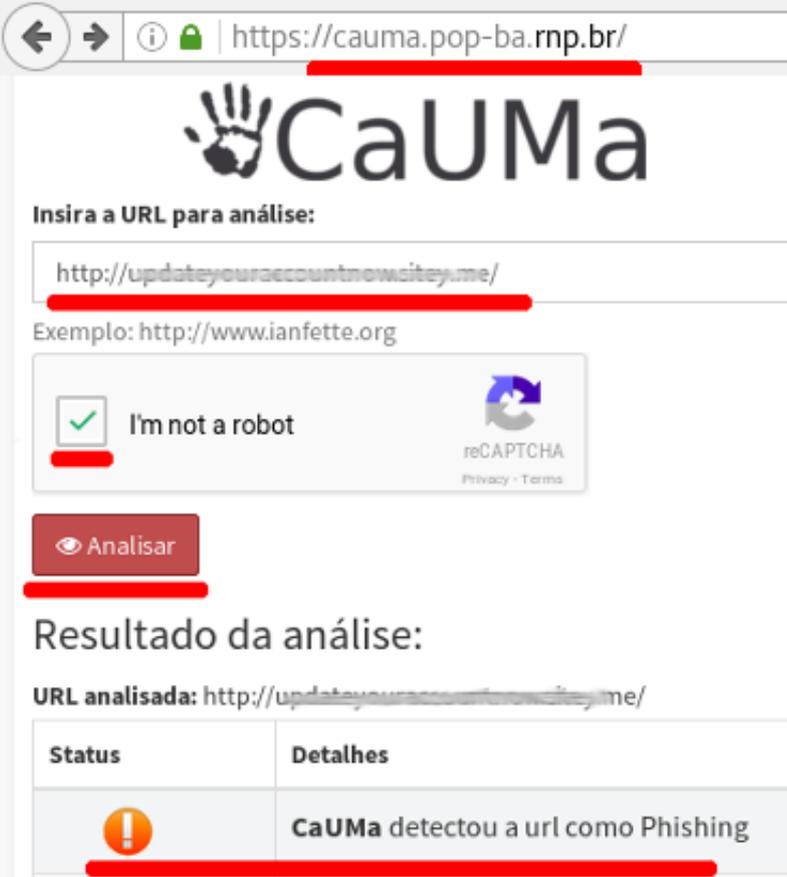


Conscientização

- Esforços devem ser direcionados em:
 - 1) políticas, normas e procedimentos
 - 2) ferramentas, tecnologias
 - 3) pessoas (treinamento e conscientização)
- Planejar estratégias de comunicação
 - Não apenas palestra, não apenas e-mail
 - Entender a cultura organizacional
 - Avaliar o nível de maturidade em SI dos usuários
 - Aplicar o PDCA

Cauma

- Sistema desenvolvido pelo PoP-BA e UFBA para análise de links maliciosos
- Cliente web
- Integração com e-mail



The screenshot shows the CaUMA web interface. At the top, the browser address bar displays the URL <https://cauma.pop-ba.rnp.br/>. The page features the CaUMA logo, which includes a hand icon. Below the logo, there is a section titled "Insira a URL para análise:" with a text input field containing the URL <http://updateyouraccountnowsitey.me/>. An example URL is provided below: "Exemplo: <http://www.ianfette.org>". A reCAPTCHA "I'm not a robot" widget is present, with a green checkmark indicating it is completed. A red "Analisar" button is located below the input field. The "Resultado da análise:" section shows the analyzed URL: "URL analisada: <http://updateyouraccountnowsitey.me/>". Below this is a table with two columns: "Status" and "Detalhes".

Status	Detalhes
	CaUMa detectou a url como Phishing

TLS everywhere

- Modelo de ataques contra confidencialidade e autenticidade
 - Apenas 1% dos sites oferecem conteúdo HTTPS
 - Site possui HTTPS, mas usuário digita HTTP
 - Referência a conteúdos externos (ex: js)
- Soluções:
 - RNP ICPEdu – Certificado TLS
 - Projeto TLS everywhere
 - Let's Encrypt

Mozilla Observatory

- <https://observatory.mozilla.org>

OBSERVATORY
by mozilla

[Home](#) [FAQ](#) [Statistics](#) [About ▾](#)

HTTP Observatory

TLS Observatory

SSH Observatory (Beta)

Third-party Tests

Scan Summary

	Host:	██████████
	Scan ID #:	8715323
	Start Time:	September 29, 2018 10:13 AM
	Duration:	6 seconds
	Score:	0/100
Tests Passed:	6/11	

Recommended Change

[Initiate Rescan](#)

Fantastic work using HTTPS! Did you know that you can ensure users never visit your site over HTTP accidentally?

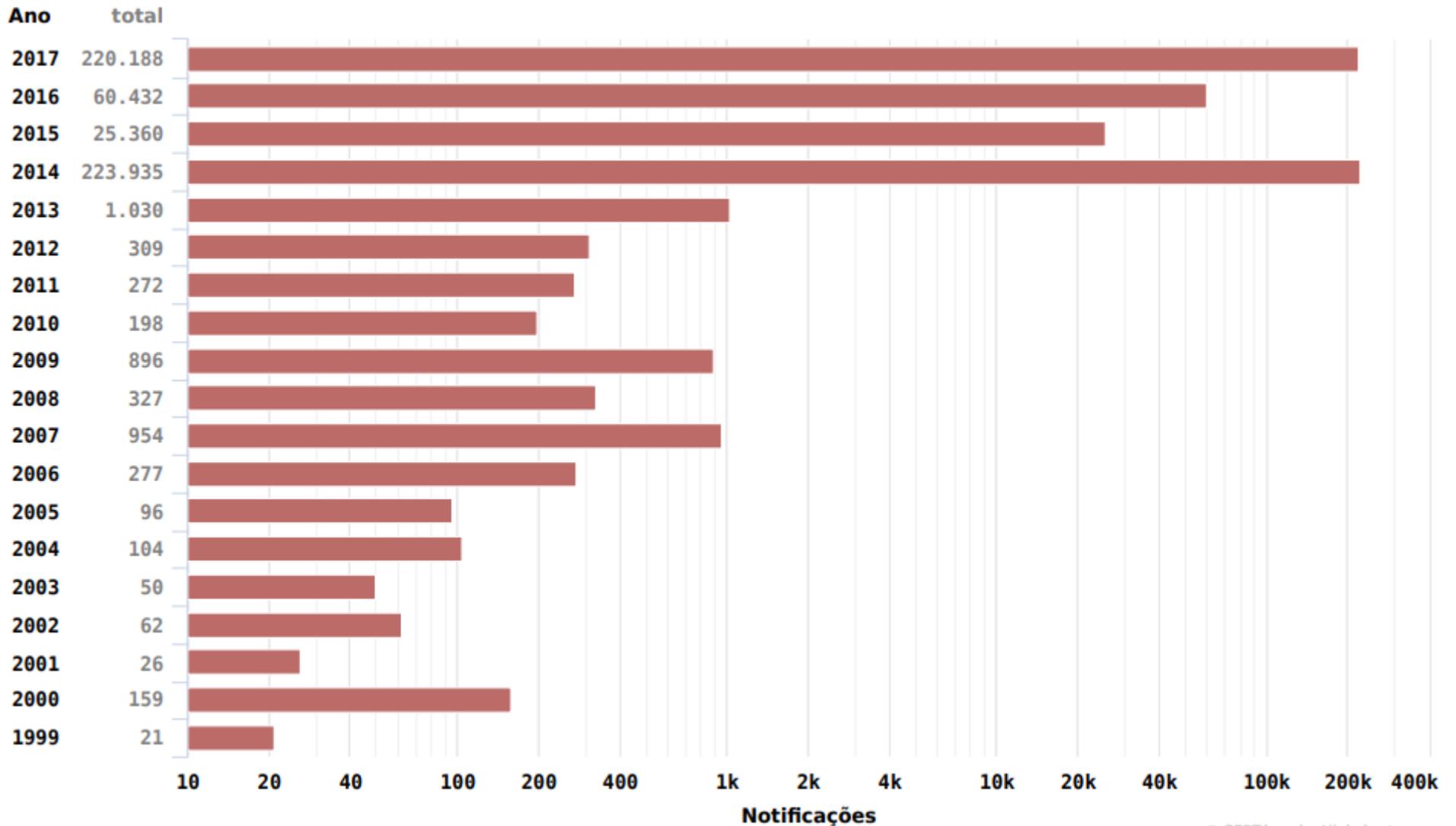
HTTP Strict Transport Security tells web browsers to only access your site over HTTPS in the future, even if the user attempts to visit over HTTP or clicks an `http://` link.

- [Mozilla Web Security Guidelines \(HSTS\)](#)
- [MDN on HTTP Strict Transport Security](#)

Once you've successfully completed your change, click [Initiate Rescan](#) for the next piece of advice.

Negação de Serviço

Notificações sobre equipamentos participando em ataques DoS



Negação de Serviço

- Crescimento e diversidade de ataques DdoS
 - Protocolos baseados em UDP (amplificação)
 - Falta de mecanismos anti-spoofing
 - Falta de ferramentas de monitoramento
 - Dificuldade de contenção

Negação de Serviço

- Protocolos baseados em UDP (amplificação)
 - Hardening de serviços (ex: DNS)
 - Firewall na borda (ex: snmp, ntp, etc)
 - Tratamento de Vulnerabilidades
- Falta de mecanismos anti-spoofing
 - Filtros de saída
 - BCP 38 (Campanha Anti-Spoofing CAIS/RNP)

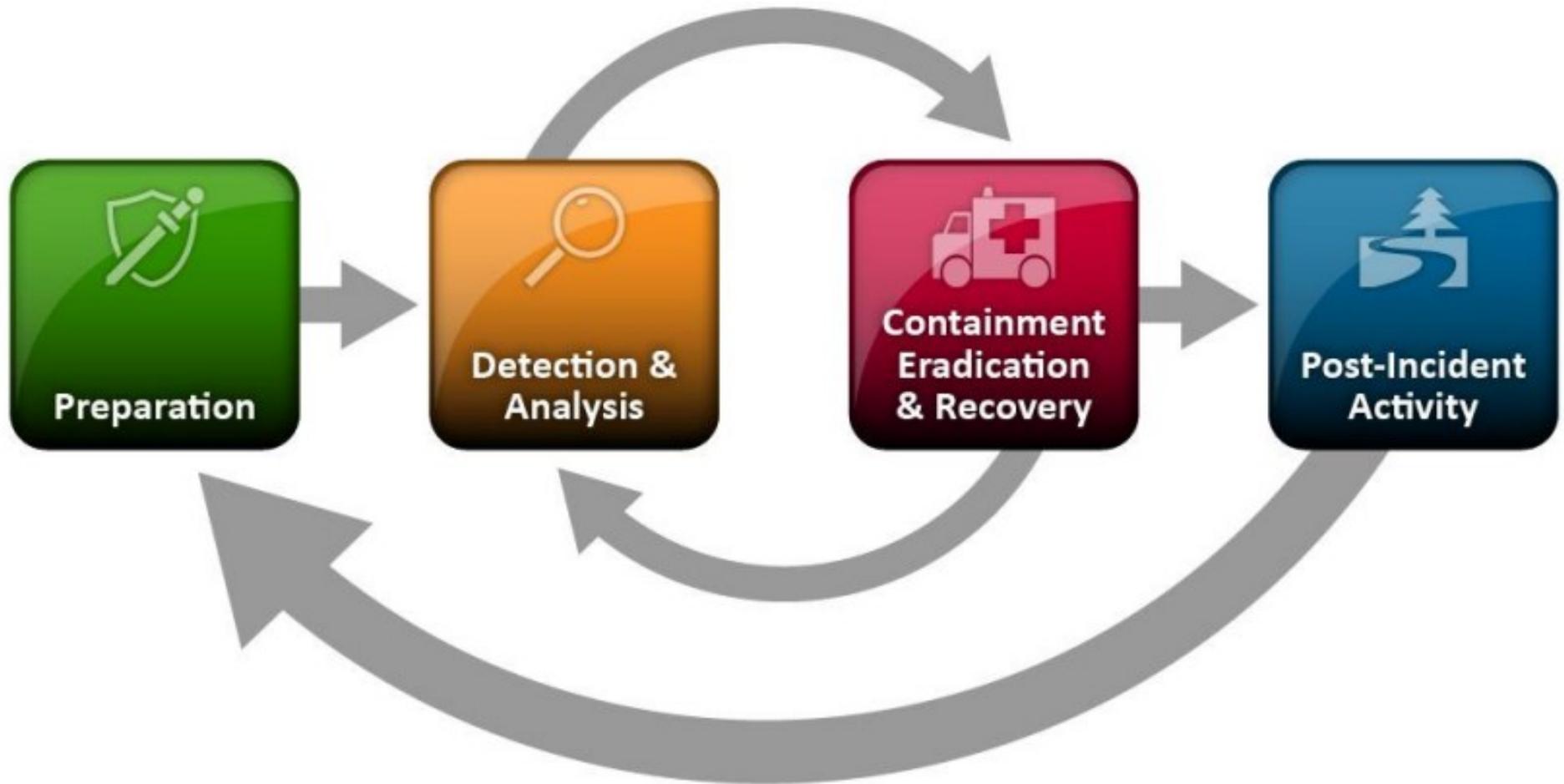
Negação de Serviço

- Falta de ferramentas de monitoramento
 - Sensores de Segurança do CAIS/RNP
 - Fluxos de Rede + Network profiling
- Dificuldade de contenção
 - Mapear estratégias de contenção
 - Plano de comunicação emergencial upstream
 - Tratar incidentes internos

Tratamento de Incidentes

- Exemplos:
 - Hosts infectados com malware
 - SPAM / Contas comprometidas
 - Desfiguração de página web
 - Violação de Copyright
 - Hosts explorado como origem de phishing e DoS

Tratamento de Incidentes



Tratamento de Incidentes

- Preparação:
 - Capacitação do CSIRT
 - ESR/RNP, CERT.br, NEXT STI/UFBA
 - Registro de eventos (logs)
 - Syslog (+ sflow/netflow, L2M, SIEM, ELK, ...)
 - Ferramentas
 - TRAIRA (+ Análise Forense, Backup, ...)
 - Políticas, Normas e Termos de Uso
 - Política de Segurança, AUP assinada, Termo de confidencialidade



Tratamento de Incidentes

- Falhas na preparação podem comprometer todo o processo
 - Evidências insuficientes
 - Responsabilização incorreta
 - Desempenho da equipe
 - ...

Para todo problema complexo,
existe uma solução rápida,
simples e...

Para todo problema complexo,
existe uma solução rápida,
simples e...

errada!

Cuidado com medidas simplórias

- “Bloqueia tudo, filtra rede social, limita banda!”
- “Mudança de senha a cada 3 meses, 1º dia útil do mês, 12 caracteres”
- “Reportamos 30 incidentes por dia!!! Cobramos resposta 24h depois!”

Cuidado com medidas simplórias

- “O processo tem que ser complexo, burocrático, inflexível”
- “Vamos fazer nossa própria criptografia!”
- “Nosso código/processo é fechado, não precisamos de auditoria”

Considerações finais

- Temos que atuar nas questões fundamentais como conscientização, cooperação e capacitação
- Soluções de segurança são caras e complexas, porém existem muitas ferramentas abertas
- Atenção com boas práticas, normas, legislação, fóruns políticos
- Tratar o usuário como parceiro, atuar como facilitador
- Estabelecer colaborações (experiências, auditoria ferramentas, capacitação, ...)

Obrigado!!!
;-)

Perguntas?



Italo Valcy
italovalcy@ufba.br