UFBA	**X WTR do PoP-BA/RNP** Ponto de Presença da RNP na Bahia Universidade Federal da Bahia Instrutores: Italo Valcy e Gildásio Júnior	PoP-BA Ponto de Presença da RNP na Bahia

BELLA
Building the Europe Link to Latin America

Conectando la investigación y educación europea y latinoamericana

Curso: Tratamento de Incidentes de Segurança da Informação
Prática 01: Fundamentos do Tratamento de Incidentes

Este roteiro de atividades visa exercitar os fundamentos do tratamento de incidentes de segurança e estabelecimento de CSIRTs

Parte 01: Estabelecimento de CSIRTs

Nesta atividade a turma será dividida em grupos de 3 ou 4 pessoas, ou outra quantidade definida pelos instrutores, e cada grupo atuará no estabelecimento de um CSIRT de um dos seguintes setores:

- CSIRT de universidade
- CSIRT bancário
- CSIRT do PoP-BA
- CSIRT de empresa de outsourcing de TI
- CSIRT de empresa de e-commerce
- CSIRT nacional

1. Defina o nome e sigla do CSIRT

2. Defina a Missão e Constituency

3. Defina os serviços ofertados pelo CSIRT

4. Defina a taxonomia de incidentes

Parte 02: Tratamento de Incidentes

Considere que a sua organização é uma Faculdade FAFUQ é detentora do DNS fafuq.com.br e da faixa de endereços 203.0.113.0/24.

1. De acordo com a taxonomia de incidentes definida na parte 01, categorize os incidentes abaixo:

a) Uma ligação telefônica para o diretor de departamento solicitando a senha de um servidor crítico, pois o funcionário responsável está inacessível;
b) Notificação externa com título “Tentativas de acesso SSH partindo do IP 203.0.113.66”
c) Notificação externa com título “[Spamcop abuse spam report regarding 203.0.113.2 id:6163299832]” no conteúdo da mensagem era possível ver um cabeçalho SMTP e dentre outros detalhes: “Subject: Hi”, “From: Promoção de Vendas de Games Online <rh@fafuq.com.br>”
d) Notificação externa com título “[SpamCop (Spamvertised web site: http://www.fafuq.com.br/db.php?f=62&2xAw1vj&3vP=9Lv) id:6465978024]Don't W@nna be with0ut You”
e) Notificação externa com título “[CAIS #9999999] Violação de Copyright”
f) Alerta do sistema de monitoramento de segurança “19/12/2018-09:45:25; ET TROJAN JS.InfectedMikrotik Injects Domain Observed in DNS Lookup; 203.0.113.99:29382; 8.8.8.8:53; UDP”
g) Usuário envia e-mail para o CSIRT informando que a pasta da diretoria financeira no servidor de arquivos da FAFUQ está automaticamente montada nas máquinas de uso comum da recepção
h) Funcionário novo na FAFUQ enviou reclamação para o CSIRT pois, ao clicar na função de reset/lembrete de senha do sistema acadêmico de notas, recebeu no corpo do e-mail a senha que ele mesmo cadastrou anteriormente “fafuq123”
i) Um funcionário da faculdade agenda reunião com o CSIRT e leva um e-mail impresso onde ele havia recebido mensagens de ameaça e está bastante preocupado e questionando se ele deve formatar seu computador, mudar todas as senhas e procurar a polícia federal, ou outras orientações. Um trecho do e-mail contém:

```
----- Mensagem encaminhada -----
De: fulano@fafuq.com.br
Para: fulano@fafuq.com.br
Enviadas: Sexta-feira, 12 de outubro de 2018 11:54:44
Assunto: Your Account Was Hacked!

8Hello!
I'm a member of an international hacker group.

Now I have access to all your accounts!

Within a period from July 30, 2018 to October 9, 2018, you were infected by the virus we've created,
through an adult website you've visited.
So far, we have access to your messages, social media accounts, and messengers.
Moreover, we've gotten full damps of these data.

We are aware of your little and big secrets...yeah, you do have them. We saw and recorded your
doings on porn websites. Your tastes are so weird, you know..

Transfer $450 to our Bitcoin wallet: 1MN7A7QqQaAVoxV4zdjdrnEHXmjhzcQ4Bq
If you don't know about Bitcoin please input in Google "buy BTC". It's really easy.

I guarantee that after that, we'll erase all your "data"

A timer will start once you read this message. You have 48 hours to pay the above-mentioned amount.

Your data will be erased once the money are transferred.
If they are not, all your messages and videos recorded will be automatically sent to all your
contacts found on your devices at the moment of infection.
```

2. Considerando o incidente 1.b acima, quais ações de contenção poderiam ser aplicadas pelo seu CSIRT?

3. Considerando o incidente 1.d acima, quais evidências devem ser coletadas pelo seu CSIRT?

4. Considerando o incidente 1.c acima, quais ações o CSIRT da sua organização tomaria para conter e tratar esse incidente?

5. Considerando o incidente 1.i acima, quais lições aprendidas podem ser tiradas deste incidente?

6. Considerando o incidente 1.h acima, qual a criticidade o seu CSIRT atribuirá a este incidente e quais critérios foram utilizados para definir esse grau de criticidade?

Boa prática! Em caso de dúvidas, não hesite em consultar os instrutores.