

## *Insider Threats*

# Estamos convidando os inimigos a entrar?

**Miriam von Zuben**

[miriam@cert.br](mailto:miriam@cert.br)

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil  
Núcleo de Informação e Coordenação do Ponto BR  
Comitê Gestor da Internet no Brasil

# Agenda

- **Introdução**
- **Problemas causados**
  - exemplos
- **Categorias**
- **Detecção e prevenção**
- **Leituras recomendadas**

# Introdução

## O que é um *insider threat*?

***Insider threat* (“atacante interno”) é um:**

- funcionário ou ex-funcionário
- prestador de serviço, parceiro ou funcionário terceirizado
- que possui/possuiu acesso a dados, sistemas ou rede de uma organização
- que de forma intencional ou não intencional:
  - excede
  - mal utiliza
  - não utiliza esse acesso
- ocasionando no prejuízo ou na possibilidade de prejuízo de informações e sistemas desta empresa

[http://resources.sei.cmu.edu/asset\\_files/TechnicalReport/2012\\_005\\_001\\_34033.pdf](http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf)

## Principais características (1/2)

- **Estão um passo a frente em relação aos atacantes externos**
  - conhecem as “jóias da coroa”
  - possuem direito de acesso a:
    - informações, sistemas, bases de dados
- **Podem contornar mecanismos de segurança**
  - acessos legítimos
  - difíceis de serem detectados
    - envolvem fatores humanos
    - como saber se uma empresa já teve problema ou não?
    - como saber se algo não foi detectado?
- **Ataques externos X internos:**
  - externos: maior quantidade
  - internos: causam mais danos

## Principais características (2/2)

- **Motivação:**
  - **financeiras**
    - **extorsão**
  - **vingança**
  - **expectativas não atendidas**
  - **ideológicas**
  - **conluio com *underground* ou crime organizado**
  - **falta de conhecimento, ingenuidade (não intencional)**

# Problemas causados

## Problemas causados por *insider threats* (1/4)

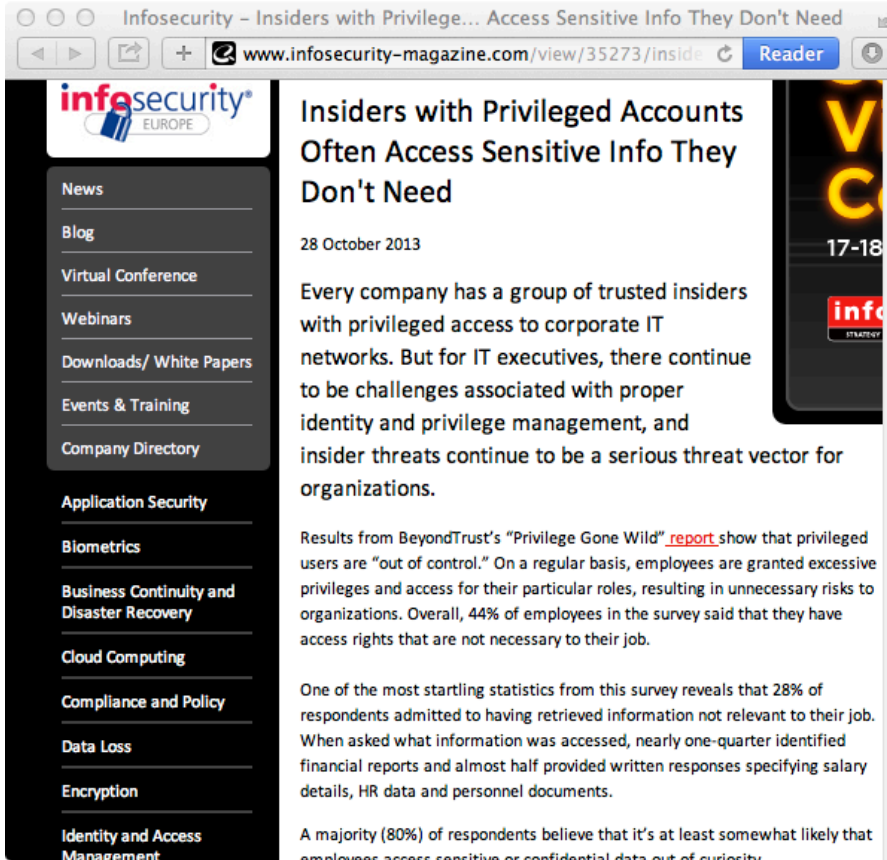
- **2013 US State of Cybercrime Survey**
  - desde, 2004, USSS, CERT-/CC, CSO Magazine, PWC
  - cerca de 600 entrevistados
  - **53% tiveram problemas com *insider threats***
  - **53% tiveram problemas mais graves com *insider threats* do que com ataques externos**
  - **incidentes mais comuns**
    - **Exposição não intencional de dados privados ou sensíveis – 34%**
    - **Furto de propriedade intelectual – 34%**
    - **Acesso não autorizado a informações, sistemas e redes – 30%**
    - **Furto de informações de clientes ou financeiras – 31%**
  - **82% resolveram os problemas internamente**

<http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-state-of-cybercrime.jhtml>

[http://resources.sei.cmu.edu/asset\\_files/Presentation/2013\\_017\\_101\\_58739.pdf](http://resources.sei.cmu.edu/asset_files/Presentation/2013_017_101_58739.pdf)



# Problemas causados por *insider threats* (2/4)

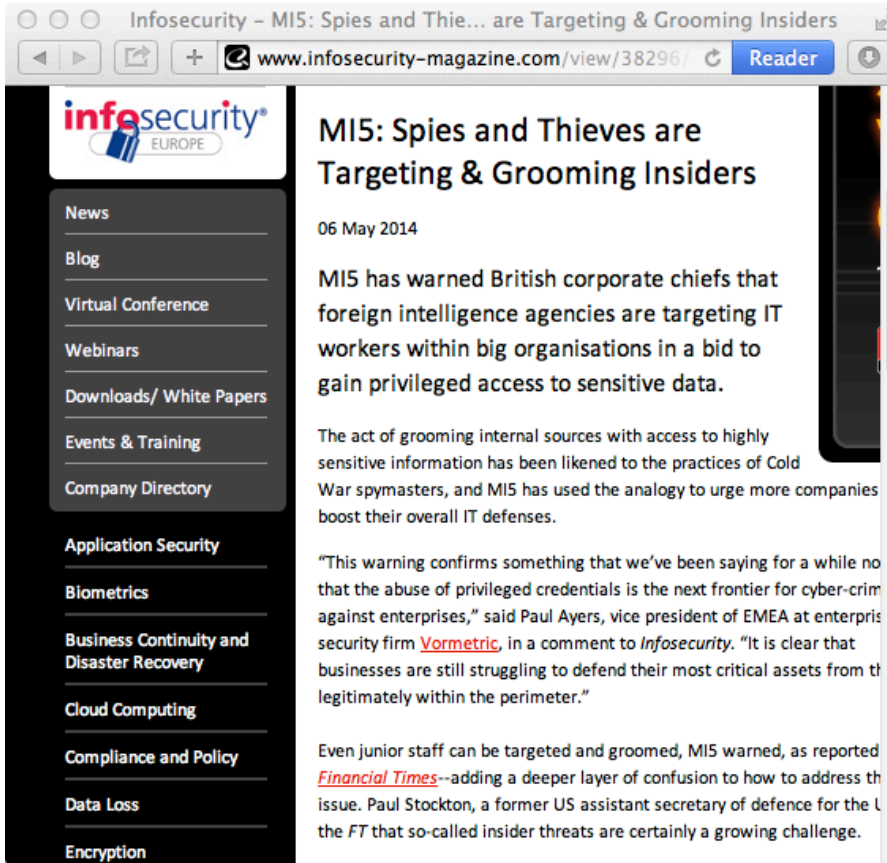


2013

- ***Privilege Gone Wild Report – BeyondTrust***
  - **28% acessaram informações não relevantes ao trabalho**
    - **relatórios financeiros, salários, RH, docs pessoais**
  - **65% das empresas possuem mecanismos de controle**
    - **54% sabem como despistá-los**
  - **44% possuem acessos desnecessários**

<http://www.infosecurity-magazine.com/view/35273/insiders-with-privileged-accounts-often-access-sensitive-info-they-dont-need/>

# Problemas causados por *insider threats* (3/4)



## 2014

- **Reporte do MI5**
- **empresas estrangeiras de inteligência visando profissionais de TI para obter dados sensíveis**
- ***“the abuse of privileged credentials is the next frontier for cyber-crime against enterprises” – Paul Ayers, vice presidente da EMEA***

<http://www.infosecurity-magazine.com/view/38296/mi5-spies-and-thieves-are-target>

## Problemas causados por *insider threats* (4/4)

- ***Cloud Computing***
- ***The Notorious Nine - Cloud Computing Top Threats in 2013*** –
  - **Acesso de informações**
    - quem possui acesso?
    - informações criptografadas?
    - quem possui acesso às chaves?

[https://downloads.cloudsecurityalliance.org/initiatives/top\\_threats/  
The\\_Notorious\\_Nine\\_Cloud\\_Computing\\_Top\\_Threats\\_in\\_2013.pdf](https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf)

# Exemplos

## Exemplos de *insider threats* (1/6)

- **Difíceis de serem achados**
- **Organizações não tornam casos públicos**
  - **problemas são tratados internamente**
    - falta de evidências e provas
    - dano insuficiente
    - dificuldade de identificar o(s) autor(es)
    - preocupação com publicidade negativa
- **EUA: leis obrigando empresas a notificarem vazamento de informações de identificação pessoal**

# Exemplos de *insider threats* (2/6)

Planalto se cala sobre espião preso após roubar informações dos colegas – Política – Correio Braziliense

www.correiobraziliense.com.br/app/noticia/

Planalto se cala sobre espião preso após roubar informações dos colegas – Polític...

## Planalto se cala sobre espião preso após roubar informações dos colegas

João Valadares  
Publicação: 21/09/2012 07:46 Atualização:



Prisão do funcionário que invadiu e-mails da agência de informações irritou o governo, que trata o assunto com sigilo

O episódio da prisão em flagrante W.T.N., de 35 anos, servidor da Agência Brasileira de Inteligência (Abin) que conseguiu "hackear" 238 senhas de investigadores do órgão, está sendo tratado pela Presidência da República com absoluto sigilo. Um dia depois de o Correio revelar que o oficial técnico de inteligência foi preso em flagrante, dentro de sua sala na própria instituição, o Gabinete de Segurança Institucional (GSI) se fechou para não expor ainda mais a fragilidade da proteção de informações sigilosas. Ontem, o ministro chefe do GSI, general José Elito Carvalho, tratou do assunto em várias reuniões. Para auxiliares, o ministro demonstrou grande insatisfação com a divulgação do caso.

Leia mais notícias em Política

O Correio apurou que o espião W.T.N. foi

## 2009

- **Funcionário da Abin**
- **238 senhas *hackeadas***
- **detectado por um “fluxo atípico de dados em uma estação de trabalho”**

[http://www.correiobraziliense.com.br/app/noticia/politica/2012/09/21/interna\\_politica,323675/planalto-se-cala-sobre-espiao-preso-apos-roubar-informacoes-dos-colegas.shtml](http://www.correiobraziliense.com.br/app/noticia/politica/2012/09/21/interna_politica,323675/planalto-se-cala-sobre-espiao-preso-apos-roubar-informacoes-dos-colegas.shtml)

## Exemplos de *insider threats* (3/6)

G1 - Detran-AM descobre programa espião... estagiários - notícias em Trânsito AM

G1 - Detran-AM descobre programa espião em sistema e afasta estagiários - notícias em Trânsito AM

25/02/2014 22h25 - Atualizado em 25/02/2014 22h25

### Detran-AM descobre programa espião em sistema e afasta estagiários

Software espião foi instalado em computadores do órgão, diz Detran. Três estagiários são suspeitos de receberem R\$ 500 por ação realizada.

Marcos Dantas e Leandro Tapajós  
Do G1 AM

3 comentários  31  62



Leonel Feitoza confirmou o descobrimento da fraude (Foto: Reprodução/TV Amazonas)

Três estagiários, dos cursos de direito e tecnologia da informação, que atuavam no Departamento de Trânsito do Estado do **Amazonas** (Detran/AM) são suspeitos de participarem de um esquema de fraudes. Segundo informações do órgão, o trio teria implantado um software 'espião' que permitia realizar alterações em processos. Eles supostamente recebiam cerca de R\$ 500 por ação realizada, entre elas a retirada de pontos de Carteiras Nacionais de Habilitação (CNHs). O esquema foi descoberto no fim de janeiro. Os suspeitos foram indiciados nessa segunda-feira (24) e devem responder por corrupção passiva. As informações sobre a fraude foram divulgadas à imprensa nesta terça-feira (25).

### 2014

- Detran – AM
- Instalação de *spyware*
- Fraude:
  - retirada de pontos de CNH

<http://g1.globo.com/am/amazonas/transito/noticia/2014/02/detran-am-descobre-programa-espiao-em-sistema-e-afasta-estagiarios.html>

# Exemplos de *insider threats* (4/6)

**Navy Systems Admin. Faces Hacking Charge**  
Allegedly Hacked Computer Systems of 30 Organizations

By Jeffrey Roman, May 6, 2014. Follow Jeffrey @gen\_sec

Credit Eligible | Email | Tweet | Like | Share | Get Permission

A former systems administrator in the nuclear reactor department of an aircraft carrier is one of two individuals charged with hacking **U.S. Navy** computer systems and those at dozens of other government and commercial organizations.

The U.S. Attorney's Office for the Northern District of Oklahoma alleges that Nicholas Paul Knight of Chantilly, Va., and Daniel Trenton Krueger of Salem, Ill, conspired to hack computers and systems as part of a plan to steal identities, obstruct justice and damage a protected computer.

At the time of the hacking attacks, Knight was assigned to the nuclear aircraft carrier USS Harry S. Truman as a systems administrator in the nuclear reactor department. Krueger was a student at an Illinois community college where he studied network administration, prosecutors say.

Knight and Krueger were members of the hacking group Team Digi7al, the U.S. attorney's office alleges. Knight allegedly served as the group's self-proclaimed leader and publicist.

In June 2012, the Naval Criminal Investigative Service detected a **breach** of the Navy's Smart Web Move database. The database manages transfers for service members of all branches of the military, storing sensitive personal records, including Social Security numbers, names and dates of birth, for approximately 220,000 service members.

## 2014

- **Administrador de redes**
- **Alvo: Marinha americana e diversas empresas**
- **Objetivo:**
  - **furtar dados pessoais**
  - **danificar computador protegido**
- **Informações coletadas postadas via Twitter**
- **Membro do grupo *hacker* Team Digi7al**

<http://www.govinfosecurity.com/navy-systems-admin-faces-hacking-charge-a-6816>



## Exemplos de *insider threats* (5/6)



### 2013

- **Edward Snowden**
  - vazamento de informações
  - abuso dos privilégios de administrador
  - uso de senhas de colegas de trabalho

[http://www.computerworld.com/s/article/9243915/Snowden\\_serves\\_up\\_another\\_lesson\\_on\\_insider\\_threats](http://www.computerworld.com/s/article/9243915/Snowden_serves_up_another_lesson_on_insider_threats)

## Exemplos de *insider threats* (6/6)



### 2008

- **Administrador era o único a possuir a senha de acesso ao roteador**
- **insubordinação**

<http://www.govinfosecurity.com/navy-systems-admin-faces-hacking-charge-a-6816>

# Categories

**Fonte: The CERT Guide to Insider Threats**

**<http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310>**

## categorias (1/5)

### Sabotagem

- **Causar danos à organização**
- **Perfil:**
  - **posições técnicas: administradores de redes, sistemas e dados**
  - **motivações:**
    - **descontentamento, falta de reconhecimento, sentir-se injustiçado**
  - **costumam ocorrer logo após a demissão**
    - **mas podem ter sido preparados há muito tempo**
- **Forma:**
  - **implantação de bombas lógicas (*logic bomb*)**
  - **inclusão de *backdoors* e outros *malware***
  - **mudança de senhas**
  - **exploração de vulnerabilidades**
  - **instalação de ferramentas maliciosas, de acesso remoto**
  - **desativação de *logs* e antivírus**
  - **extorsão**

## categorias (2/5)

### Fraude

- **Manipulação de dados para ganhos próprios**
- **Vazamento de dados**
- **Perfil:**
  - **funcionários ativos**
  - **durante horário de trabalho**
  - **conluio com atacantes externos**
- **Pode ficar muito tempo até ser detectado**
- **Quanto mais alto o cargo maiores podem ser os danos**

### Espionagem

- **Entre países e empresas**

## categorias (3/5)

### Furto de propriedade intelectual

- **Espionagem industrial**
- **Informações furtadas para:**
  - conseguir novo emprego
  - abrir negócio próprio
  - vender para outras empresas
- **Envio de informações**
  - *e-mail, pen-drive, CDs*
  - acessos indevidos
  - *notebooks, dispositivos móveis*
  - ssh, ftp, telnet

## categorias (4/5)

### Não intencionais

- **Causadas por uma ação:**
  - uso de engenharia social
  - **exemplos:**
    - vazamento de informações
    - instalação de códigos maliciosos
      - *APT, malware, phishing*
    - descarte de discos, *pen-drives*, papéis
    - perda de equipamentos

## Categories (5/5)

### Não intencionais

- **Causadas por falta de ação**
  - **omissão, desleixo, falta de comprometimento**
    - **NÃO** instalação de correções de segurança
    - **NÃO** fazer *backups*
    - **NÃO** utilizar criptografia
    - **NÃO** utilizar técnicas de programação segura
    - **NÃO** configurar os sistemas corretamente
    - **NÃO** usar senhas fortes
    - **NÃO** bloquear estação de trabalho
- **BYOD, pode facilitar:**
  - vazamento de dados
  - perda de dados
  - propagação de *malware*



# Detecção e Prevenção

**Fonte: The CERT Guide to Insider Threats**

**<http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310>**

## Detecção e prevenção (1/4)

- **Empresas com dificuldade em perceber a extensão do problema**
  - preocupadas mais com ameaças externas que internas
- **Difíceis de serem prevenidos**
  - atacantes exercendo ações autorizadas
  - possuem acesso legítimo a dados, sistemas e equipamentos
  - possuem conhecimento sobre sistemas, computadores, topologia, infra-estrutura, etc.
- **Apenas indicadores técnicos são insuficientes**
  - precisam ser combinados com indicadores comportamentais
- **Criar grupo multidepartamental para lidar com esses casos**
  - TI, RH, jurídico, etc
  - antecipar comportamentos negativos

## Detecção e prevenção (2/4)

- **Modo de operação:**
  - a partir do momento que um atacante externo possui acesso interno a uma rede/sistema pode agir da mesma forma que um atacante interno
  - proteção contra atacantes internos também previnem contra atacantes externos
- **Devem ser incluídos na análise de risco**
- **Definição de políticas**
  - separação de tarefas, privilégio mínimo
  - desligamento de funcionários
  - *backup* e recuperação de dados
  - *two-man rule*
  - BYOD
- **Acordos claros com serviços de *cloud computing***

## Detecção e prevenção (3/4)

- **Gerenciamento de contas e senhas**
  - controle de acesso restrito a usuários com acessos privilegiados
- **Uso de ferramentas de correlação de *logs***
- **Estabelecer o que é um comportamento “normal” de rede**
- **Controle e monitoração**
  - *logs*, auditorias, *firewall*
  - acessos remotos
  - detecção pode ocorrer via relato de outros funcionários
    - desconfiança, mudanças comportamentais
- **Ficar a atento a:**
  - redes sociais
  - *data exfiltration* (*pen-drives*, HDs, CDs)

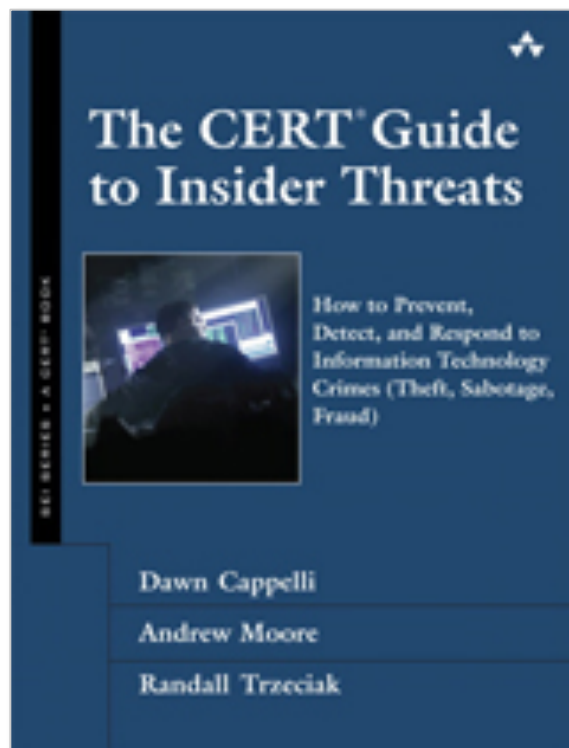
## Detecção e prevenção (4/4)

- **Não intencionais:**
  - **treinamento constante contra:**
    - engenharia social
    - *malware, phishing*
    - proteção de informações
  - **custos com treinamento e conscientização de usuários podem ser baixos se comparados com os danos que podem causados**

# Leituras Recomendadas

# The CERT Guide to Insider Threats

<http://www.cert.org/insider-threat/>



## Perguntas?

Miriam von Zuben.  
[miriam@cert.br](mailto:miriam@cert.br)

- CGI.br – Comitê Gestor da Internet no Brasil  
<http://www.cgi.br/>
- NIC.br – Núcleo de Informação e Coordenação do .br  
<http://www.nic.br/>
- CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil  
<http://www.cert.br/>
- Cartilha de Segurança para Internet  
<http://cartilha.cert.br/>



cert.br

Centro de Estudos, Resposta e Tratamento  
de Incidentes de Segurança no Brasil

nic.br

Núcleo de Informação  
e Coordenação do  
Ponto BR

egi.br

Comitê Gestor da  
Internet no Brasil



# 3º Fórum Brasileiro de CSIRTs

15 a 16 de setembro

Evento conjunto: Seminário de Proteção à Privacidade e aos Dados Pessoais

Envio de propostas até 27 de julho

The screenshot shows a web browser window with the URL [www.cert.br/forum2014/](http://www.cert.br/forum2014/). The page header includes the cert.br logo and the text "Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil". The main navigation bar features the event title "3º Fórum Brasileiro de CSIRTs" and a section for "Eventos conjuntos:" which includes "3º Fórum Brasileiro de CSIRTs" and "V Seminário de Proteção à Privacidade e aos Dados Pessoais". Below the navigation bar, there are links for "Início", "Programação", and "Inscrições". A sidebar on the left contains a menu with items: "Keynote", "Programação", "Envio de trabalhos", "Inscrições", "Local", "Hotéis", "Informações de Interesse", and "Evento conjunto: V Seminário de Proteção à Privacidade e aos Dados Pessoais". The main content area has a language selector for "English" and a section titled "Sobre o Evento" with the following text: "O Fórum Brasileiro de CSIRTs é um evento dedicado à discussão de assuntos relacionados com tratamento de incidentes e resiliência das organizações face a incidentes de segurança. O terceiro evento será realizado nos dias 15 e 16 de setembro de 2014. Haverá tradução simultânea entre Português e Inglês." Below this is a section titled "Datas Importantes" with a list of key dates:
 

- 27 de julho de 2014: Data limite para envio de propostas de palestras
- 11 de agosto de 2014: Anúncio das propostas aceitas
- 15 e 16 de setembro de 2014: 3º Fórum Brasileiro de CSIRTs
- 17 e 18 de setembro de 2014: Evento conjunto: V Seminário de Proteção à Privacidade e aos Dados Pessoais

# 3º Fórum Brasileiro de CSIRTs

3º Fórum Brasileiro de CSIRTs

Eventos conjuntos: 3º Fórum Brasileiro de CSIRTs, V Seminário de Proteção à Privacidade e aos Dados Pessoais

**Início** | **Programação** | **Inscrições**

**Submeta sua Proposta de Palestra**

Convidamos todos os profissionais atuantes em Grupos de Tratamento de Incidentes de Segurança (CSIRTs) ou que trabalhem com segurança e tratamento de incidentes no seu dia-a-dia, a submeter propostas de palestras de interesse da Comunidade de Tratamento de Incidentes no Brasil, para o 3º Fórum Brasileiro de CSIRTs, que ocorrerá nos dias 15 e 16 de setembro de 2014.

Para os trabalhos aceitos, o NIC.br proverá apoio para transporte e estadia de um profissional para apresentar o trabalho.

**Temas de Interesse**

A apresentação deve tratar de aspectos práticos e operacionais das atividades de tratamento e gestão de incidentes de segurança, bem como de aspectos da segurança da informação ou da Internet que sejam relacionados com ou tenham impacto no processo de tratamento de incidentes.

Uma sugestão de temas de interesse para este evento segue:

- Detecção de botnets, computadores e dispositivos móveis infectados
- Mitigação e remediação de botnets
- Estudos de caso relacionados a incidentes tratados
- Tendências observadas nos incidentes tratados
- Automatização de processos de tratamento de incidentes
- Segurança na Internet das Coisas
- Outros temas de interesse para CSIRTs

**Importante:** é desejável que as apresentações sejam aplicadas e \*não\* devem ser voltadas a produtos e soluções de fornecedores específicos, com fins comerciais, nem trabalhos que sejam com ênfase puramente acadêmica.

**Submissão de Trabalhos**

As propostas de trabalhos deverão ser enviadas para o e-mail: [forum@cert.br](mailto:forum@cert.br) com os seguintes dados:

- Título completo do trabalho a ser apresentado
- Resumo (Abstract) estendido, além de um rascunho dos slides ou descrição detalhada, se o tiver. O Comitê Avaliador