
egi
Escola de Governança
da Internet no Brasil

Estratégias para Tratamento e Prevenção de Incidentes de Segurança

Cristine Hoepers, D.Sc.
Klaus Steding-Jessen, D.Sc.

01/04/2016

Objetivos

Discutir como os diversos atores podem atuar de forma cooperativa para prevenir e mitigar os ataques feitos através da Internet

- De forma não exaustiva

Objetivo principal é um ecossistema saudável

Nenhum grupo ou estrutura única conseguirá fazer sozinha a segurança ou a resposta a incidentes - todos tem um papel

- desenvolvedores
  - precisam pensar em segurança desde as etapas iniciais de desenvolvimento
- gestores
  - precisam considerar segurança como um investimento e alocar recursos adequados
- administradores de redes e sistemas e profissionais de segurança
  - não emanar “sujeira” de suas redes
  - adotar boas práticas
- usuários
  - entender os riscos e seguir as dicas de segurança
  - manter seus dispositivos atualizados e tratar infecções

<u>Cooperação</u> é primordial – nacional e internacional

Ainda assim ataques e incidentes de segurança ocorrerão

Organizações Precisam Almejar Resiliência

Um sistema 100% seguro é muito difícil de atingir

Resiliência: Continuar funcionando mesmo na presença de falhas ou ataques

- **Identificar o que é crítico** e precisa ser mais protegido
- **Definir políticas** (de uso aceitável, acesso, segurança, etc)
- **Treinar profissionais** para implementar as estratégias e políticas de segurança
- **Treinar e conscientizar os usuários** sobre os riscos e medidas de segurança necessários
- **Implantar medidas de segurança** que implementem as políticas e estratégias de segurança
  - como: aplicar correções ou instalar ferramentas de segurança
- Formular **estratégias para gestão de incidentes** de segurança e formalizar **grupos de tratamento de incidentes**

Conceitos Relacionados a Gestão de Incidentes

Incidente de Segurança em Computadores – qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores

Tratamento de Incidentes – processo de identificar, mitigar e prevenir incidentes de segurança

CSIRT – acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, responsável por tratar incidentes de segurança para um público alvo específico

Outros acrônimos: IRT, CIRC, CIRT, SERT, SIRT, CERT®

No Brasil também são usados: CTIR, ETIR

Papel dos CSIRTs

A redução do impacto de um incidente é conseqüência:

- da agilidade de resposta
- da redução no número de vítimas

O papel do CSIRT é:

- auxiliar a proteção da infraestrutura e das informações
- prevenir incidentes e conscientizar sobre os problemas
- auxiliar a detecção de incidentes de segurança
- responder incidentes – retornar o ambiente ao estado de produção

O sucesso depende da confiabilidade

- nunca divulgar dados sensíveis nem expor vítimas, por exemplo

O CSIRT não é "investigador"

- foco é entender "o que" o que aconteceu, não "quem" originou a ação
  - ferramentas muitas vezes são as mesmas da investigação e da perícia
- naturalmente pode identificar possíveis crimes e então:
  - atuar na preservação de evidências
  - auxiliar investigações posteriores, dependendo de sua missão

Evolução histórica:
Tratamento de Incidentes no Brasil

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil" é publicado pelo CGI.br[1]

Junho/1997: o CGI.br cria o CERT.br (naquele tempo chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório, como um grupo com responsabilidade nacional[2]

Agosto/1997: a RNP cria seu próprio CSIRT (CAIS)[3], seguida pela rede acadêmica do Rio grande do Sul (CERT-RS)[4]

1999: outras instituições, incluindo Universidades e Operadoras de Telecomunicações, iniciaram a formação de seus CSIRTs

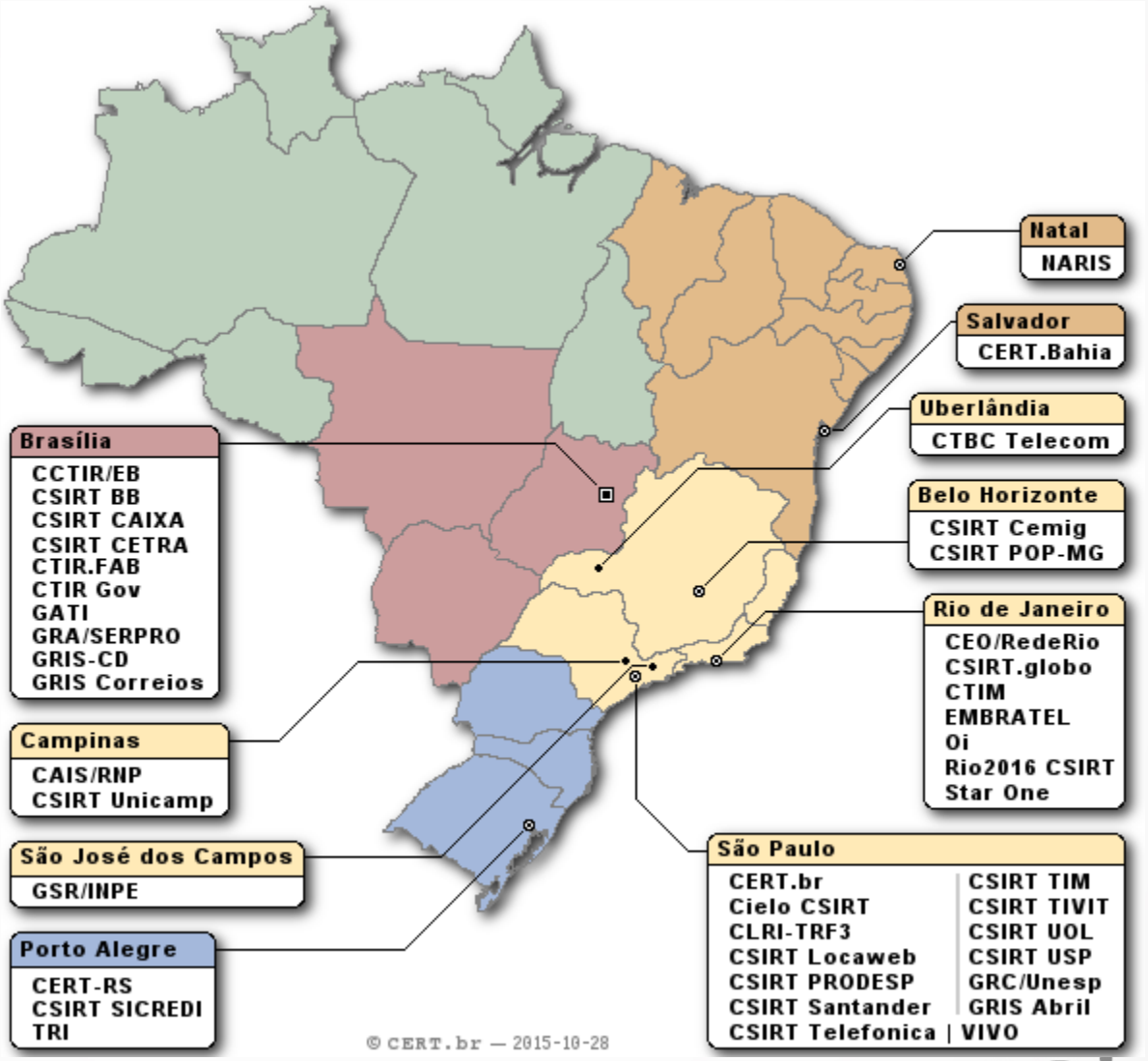
2002–2004 : grupos de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal

2004: o CTIR-Gov foi criado, com a Administração Pública Federal como seu público alvo[5]

[1] http://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169
[2] http://www.nic.br/pagina/gts/157
[3] http://memoria.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[4] http://www.cert-rs.tche.br/index.php/missao
[5] http://www.ctir.gov.br/sobre-CTIR-gov.html

Grupos de Tratamento de Incidentes Brasileiros: **41 times com serviços anunciados ao público**

Público Alvo	CSIRTs
Qualquer Rede no País	CERT.br
Governo	CTIR Gov, CCTIR/EB, CLRI-TRF-3, CSIRT PRODESP, GATI, CTIM, GRA/SERPRO, CTIR.FAB, GRIS-CD, CSIRT CETRA, GRIS Correios
Setor Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, CSIRT Telefonica|VIVO, CSIRT Locaweb, CSIRT TIM, CSIRT UOL, StarOne, Oi,
Academia	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CEO/RedeRio, CERT.Bahia, CSIRT USP, GRC/UNESP, TRI
Outros	Rio2016 CSIRT, CSIRT TIVIT, GRIS Abril, CSIRT Globo, CSIRT Cemig



http://www.cert.br/csirts/brasil/

Cenários Comuns de Ataques e Participação dos Diversos Atores para Prevenção e Mitigação

Cenário:
Ataque Contra Usuários de Internet

Usuário recebe *e-mail* com *link* para um código malicioso (*malware*)
[Usando ardis diversos, como: Ata de reunião, Intimação, Dívida em Aberto, Nota Fiscal Eletrônica, etc]

Código é baixado e executado pelo usuário, ação que infecta o dispositivo com o *malware*

O *malware* se conecta em um servidor de Comando e Controle (C&C)

Malware recebe comandos do atacante para, por exemplo:

- instalar *spyware*
- enviar e-mails para todos os contatos do usuário, com link para o *malware*
- exfiltrar dados
- enviar spam
- atacar outras redes (DDoS, invasões, etc)

Atores e Seus Papéis Para Prevenção e Mitigação das Infecções por *Malware*

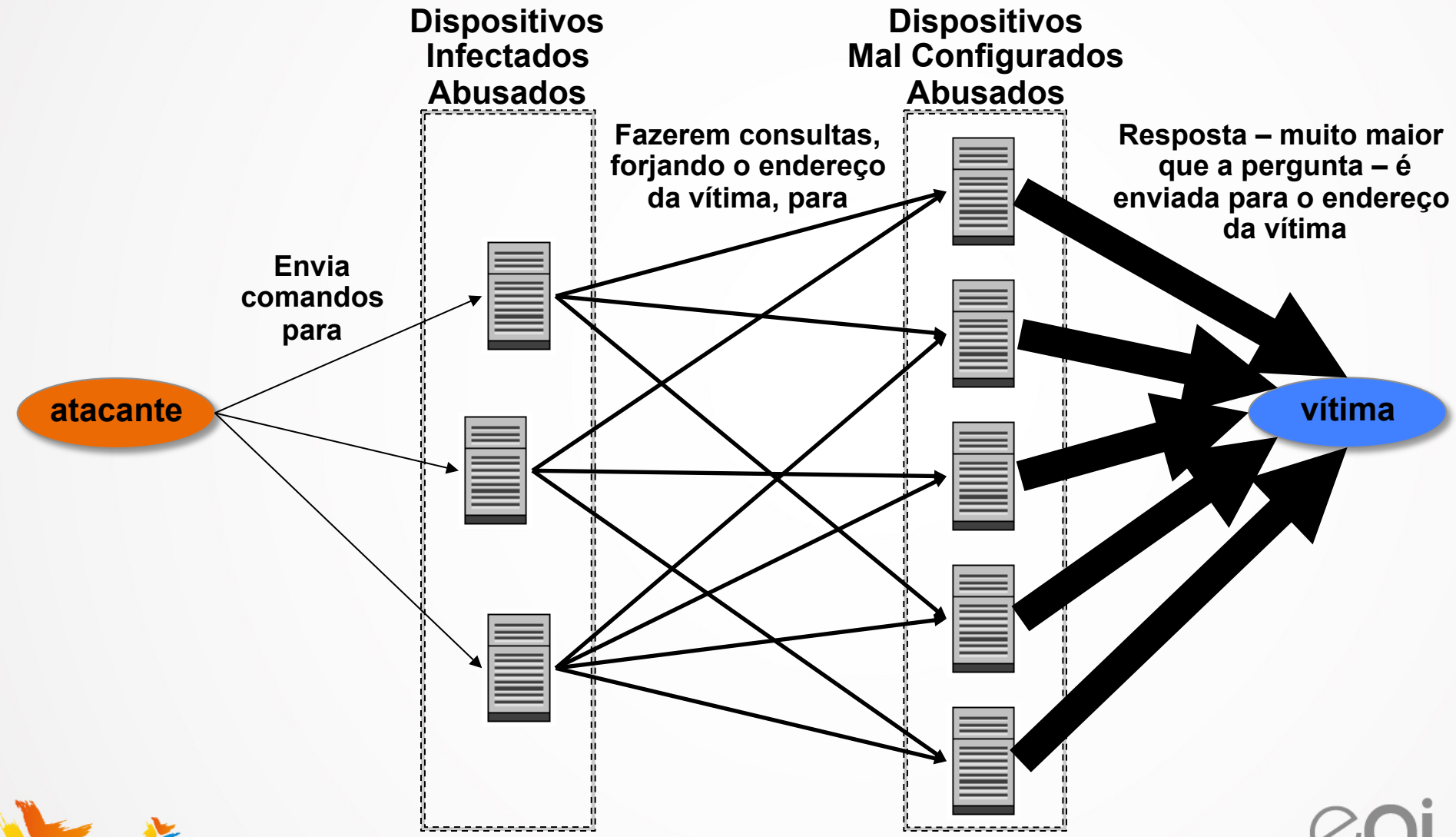
Usuários: manter sistemas atualizados, prevenir-se de infecções, “limpar” dispositivos infectados

Rede onde está hospedado o *malware ou o C&C*:

- se foi inserido por um invasor: corrigir os problemas e remover o arquivo malicioso
- se foi colocado por um cliente: aplicar as políticas de uso aceitável

Desenvolvedores de sistemas: desenvolver sistemas com configurações padrão mais seguras

Anatomia de um Típico Ataque de Negação de Serviço (DDoS)



Atores e Seus Papéis na Redução dos Ataques de Negação de Serviço (DDoS)

Boas práticas para reduzir o "poder de fogo":

- **Detentores de AS:** implementar *anti-spoofing* (BCP 38)
- **Provedores de Serviços:** (NTP, DNS, etc): configurar corretamente os serviços para evitar amplificação
- **Usuários:** manter sistemas atualizados, prevenir-se de infecções, "limpar" dispositivos infectados;
- **Desenvolvedores de sistemas:** desenvolver sistemas com configurações padrão mais seguras

Prevenção por parte das vítimas de DDoS:

- Aumentar os recursos (mais banda, processamento, disco)
- Usar serviços ou ferramentas de mitigação

Conscientização e Fóruns de Cooperação

Cartilha de Segurança para Internet

Conteúdo disponível *online* gratuitamente sob Licença *Creative Commons*

- **Livro (PDF e ePub) e conteúdo no *site* (HTML5)**
- **Dica do dia no *site*, via *Twitter* e RSS**
- **Impressões em pequena escala enviadas a escolas e centros de inclusão digital**
- **Uso por instituições para treinar funcionários**

http://cartilha.cert.br/

Fascículos da Cartilha de Segurança para Internet

Organizados de forma a facilitar a difusão de conteúdos específicos:

- Redes Sociais
- Senhas
- Comércio Eletrônico
- Privacidade
- Dispositivos Móveis
- *Internet Banking*
- Computadores
- Códigos Maliciosos
- Verificação em Duas Etapas
- Redes

Acompanhados de *slides* de uso livre para:

- ministrar palestras e treinamentos
- complementar conteúdos de aulas

Outros Materiais para Usuários Finais

Portal Internet Segura

- Reúne todas as iniciativas conhecidas de educação de usuários no Brasil, que possuam material *online*

http://www.internetsegura.br/

INTERNET SEGURA.BR

Site e vídeos do Antispam.br

http://www.antispam.br/

Fóruns de Cooperação entre CSIRTs

Fórum Brasileiro de CSIRTs

- Evento anual para promover troca de experiências e cooperação entre CSIRTs brasileiros

Reuniões periódicas entre grupos de setores específicos

- ex: Financeiro, Governo, Telecomunicações

LAC-CSIRTs

- Reunião de Grupos de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e o Caribe

Annual National CSIRTs Meeting

- Organizado pela *CERT Division of the SEI/CMU*

FIRST (Forum of Incident Response and Security Teams)

- **Criação**: 1990
- **Membros**: 345 CSIRTs, de 74 países, participantes de todos os setores;

Outros Fóruns Internacionais de Segurança

APWG – (originalmente *AntiPhishing Working Group*)

- **Criação:** 2003
- **Membros:** 2000 organizações, participantes de todos os setores, incluindo organizações internacionais;

M³AAWG – *Messaging, Mobile, Malware Anti-Abuse Working Group*

- **Criação:** 2004
- **Membros:** Indústria – "*Internet Service Providers (ISPs), telecomm companies, Email Service Providers (ESP), social networking companies, leading hardware and software vendors, major brands, major antivirus vendors and numerous security vendors*"

Questões Emergentes

Controle vs. Segurança

Supostas medidas de segurança, mas usadas para controle, podem gerar reações contra a segurança como um todo

- uso indiscriminado da biometria em escolas, academias, acesso a edifícios, etc
- RFID (*Radio Frequency Identification*) em carros, cartões de crédito e passaportes
- portarias remotas e câmeras de segurança

Quem tem acesso? Com que finalidade?

Como estes dados estão protegidos?

Seu uso traz mesmo mais segurança no contexto em que estão sendo usados?

- estas questões também se aplicam a portarias remotas e câmeras de segurança

Internet das Coisas (IoT)

As “coisas” já estão conectadas

- carros, lâmpadas, TVs, equipamentos médicos
- são sistemas complexos e completos (tem um sistema operacional, aplicações Web, permitem acesso remoto, etc)

Mas não estão sendo tomados cuidados de segurança no projeto, implementação e adoção, vide:

- Lâmpadas *Phillips Hue LED* (criptografia fraca permite descobrir senha do wi-fi; vulnerabilidades permitem controlar remotamente)
- TVs Samsumg mandam todo o som ambiente para sede; TVs da LG enviam nomes de arquivos, filmes, inclusive dos drives de rede, que são ativamente procurados pela TV
- Carros da *Fiat Chrysler* permitindo controle do veículo via 3G/4G, via vulnerabilidades do sistema de entretenimento Uconnect
- Aviões potencialmente vulneráveis via sistemas de entretenimento
- Dispositivos médicos

Infusion Pumps

www.hospira.com/en/products_and_services/infusion_pumps

Reader

SMART OPTIONS FOR RELIABLE MEDICATION DELIVERY

Hospira high-performance infusion pumps make it easy for you to deliver exceptional patient safety and care. Our focused portfolio features proven, innovative smart pump and pain management technology designed to help meet your clinical safety and workflow goals. The powerful Hospira MedNet™ safety software helps to reduce medication errors and raise the bar for your medication management system. And, with an eye to the future, our Plum™ family of smart pumps with Hospira MedNet are designed to integrate with your electronic medical record (EMR) systems through our IV Clinical Integration solution.

Our focused line of infusion systems includes general infusion and pain management pumps:

Contact Hospira

PLUM 360™ INFUSION SYSTEM

Your direct connection to clinical excellence with integrated safety and efficiency at every step.

Advisory (ICSA-15-161-01)

More Advisories

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities

Original release date: June 10, 2015 | Last revised: June 12, 2015

STACK-BASED BUFFER OVERFLOW[b]

The researcher has evaluated the device and asserts that the device contains a buffer overflow vulnerability that could be exploited to allow execution of arbitrary code on the device. This vulnerability has not been validated by Hospira. However, acting out of an abundance of caution, ICS-CERT is including this information to enhance healthcare providers' awareness, so that additional monitoring and controls can be applied.

CVE-2015-3955[c] has been assigned to this vulnerability. A CVSS v2 base score of 7.6 has been assigned; the CVSS vector string is (AV:N/AC:H/Au:N/C:C/I:C/A:C).[d]

IMPROPER AUTHORIZATION[e]

The communication module gives unauthenticated users root privileges on Port 23/TELNET by default. An unauthorized user could issue commands to the pump.

CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

INSUFFICIENT VERIFICATION OF DATA AUTHENTICITY[h]

The device accepts drug libraries, firmware updates, pump commands, and unauthorized configuration changes from unauthenticated devices on the host network. The device listens on the following ports: Port 20/FTP, Port 23/TELNET, Port 80/HTTP, Port 443/HTTPS, and Port 5000/UPNP. Hospira has not validated claims of firmware updates and pump commands for Plum A+ and Plum A+3 from unauthorized devices on the host network.

Referências:
Fontes dos Conceitos Apresentados

Cartilha de Segurança para a Internet, ISBN: 978-85-60062-54-6

http://cartilha.cert.br/

The Importance of a Multistakeholder Approach to Cybersecurity Effectiveness

http://content.netmundial.br/contribution/the-importance-of-a-multistakeholder-approach-to-cybersecurity-effectiveness/180

Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Portal de Boas Práticas para a Internet no Brasil

http://bcp.nic.br/

Obrigado

Cristine Hoepers, D.Sc.
cristine@cert.br

Klaus Steding-Jessen, D.Sc.
jessen@cert.br

nic.br cgi.br

www.nic.br | www.cgi.br