
egi
Escola de Governança
da Internet no Brasil

Fundamentos de Segurança da Informação

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

19/08/2015 – 10:30 às 12:00h

Objetivos

Discutir os conceitos técnicos relacionados com segurança, privacidade e resiliência

De forma não exaustiva

Subsidiar os participantes para as crescentes discussões sobre privacidade, segurança, estabilidade e resiliência nos fóruns nacionais e internacionais de governança da Internet

Embasamento técnico para identificar e questionar falácias, mitos e artigos não embasados

Segurança e Governança da Internet

egi

WSIS:
Declaration of Principles

Document WSIS-03/GENEVA/DOC/4-E

12 December 2003

[...]

B5) Building confidence and security in the use of ICTs

35. Strengthening the trust framework, **including information security and network security, authentication, privacy and consumer protection**, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs.

[...]

http://www.itu.int/wsis/docs/geneva/official/dop.html

CGI.br:
Princípios para a Governança e Uso da Internet no Brasil

CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL

Fevereiro de 2009

[...]

8. Funcionalidade, segurança e estabilidade
A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa **através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas**.

[...]

http://www.cgi.br/resolucoes/documento/2009/003

NETmundial:
Internet Governance Principles

NETmundial Multistakeholder Statement

April, 24th 2014, 19:31 BRT

[...]

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a **secure, stable, resilient, reliable and trustworthy network**. **Effectiveness** in addressing risks and threats to security and stability of the Internet **depends on strong cooperation among different stakeholders**.

[...]

http://www.netmundial.org/references/

Segurança da Informação

egi

Propriedades da Segurança da Informação

Confidencialidade – é a necessidade de garantir que as informações sejam divulgadas somente para aqueles que possuem autorização para vê-las.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e lê todas as informações contidas na sua declaração de Imposto de Renda

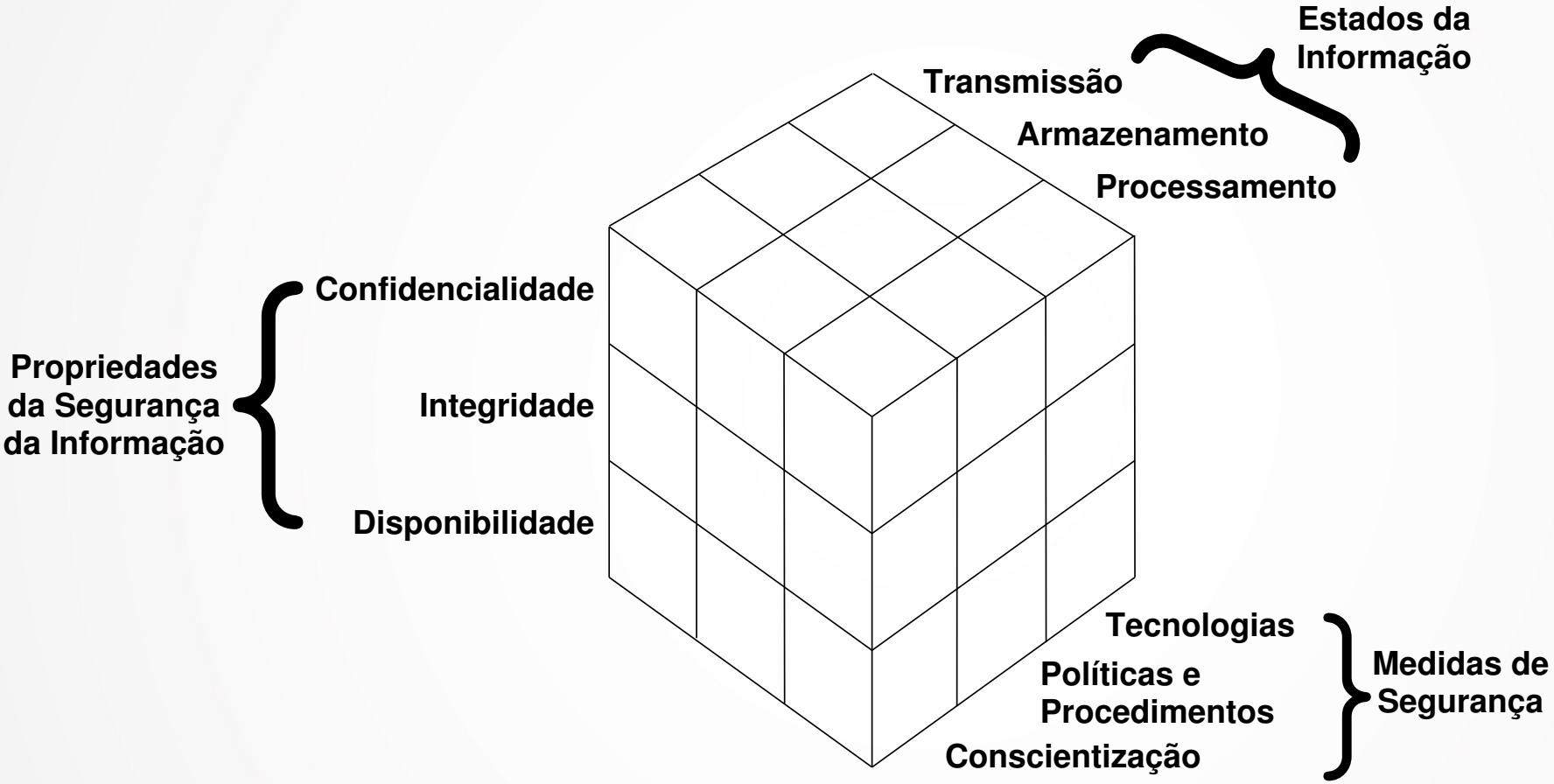
Integridade – é a necessidade de garantir que as informações não tenham sido alteradas acidentalmente ou deliberadamente, e que elas estejam corretas e completas.

Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

Disponibilidade – é a necessidade de garantir que os propósitos de um sistema possam ser atingidos e que ele esteja acessível àqueles que dele precisam.

Ex. de quebra: o seu provedor sofre uma grande sobrecarga de dados ou um ataque de negação de serviço e por este motivo você fica impossibilitado de enviar sua declaração de Imposto de Renda à Receita Federal.

As informações estão em diversos locais e a segurança depende de múltiplos fatores



McCumber Information Security Model
http://www.ibm.com/developerworks/security/library/s-confnotes2/

Privacidade vs. Confidencialidade

Do ponto de vista de Segurança da Informação:

Privacidade – habilidade e/ou direito de proteger suas informações pessoais, extende-se à habilidade e/ou direito de prevenir invasões do seu espaço pessoal.

Confidencialidade – envolve a obrigação de proteger os segredos de outras pessoas ou organizações, se você souber deles.

Riscos em Sistemas Conectados à Internet

- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- **perda de confiança na tecnologia**

Sistemas na Internet

Riscos

Atacantes

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas

Proteção de Dados via Criptografia

SSL/TLS, SSH e IPSec – protocolos que, por meio de criptografia, fornecem confidencialidade e integridade nas comunicações entre um cliente e um servidor.

VPN – termo usado para se referir à construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Em geral utilizam criptografia para proteger os dados em trânsito.

- Existem serviços na Internet que dizer fornecer uma VPN, mas que apenas fornecem serviços de *proxy* que "ocultam" o IP de origem – a maior parte destes serviços não cifra o conteúdo em trânsito.

PGP – programa que implementa operações de criptografia, como cifrar e decifrar conteúdos e assinatura digital.

- Normalmente utilizado em conjunto com programas de *e-mail*.

Registros de Eventos (*Logs*) – 1

São os registros de atividades gerados por programas e serviços de um computador. A partir da análise destas informações é possível:

- detectar problemas de *hardware* ou nos programas e serviços instalados no computador;
- detectar um ataque;
- detectar o uso indevido do computador, como um usuário tentando acessar arquivos de outros usuários, ou alterar arquivos do sistema.

Exemplos – *logs* de sistema:

```
Jul  4 10:47:01 localhost UserEventAgent[11]:
CaptiveNetworkSupport:CreateInterfaceWatchList:2788 WiFi Devices Found. :)
Jul  4 10:47:02 localhost configd[14]: network configuration changed.

Jul 28 15:07:21 notebook Software Update[443]: Can't instantiate
distribution from http://swcdn.apple.com/content/downloads/11/05/041-0925/
g27esO4pw9re5ggrfp3suf8ew6t53asfz8/041-0925.English.dist: Error
Domain=NSXMLParserErrorDomain Code=4 "zero length data"
UserInfo=0x7fed3da20e50 {NSLocalizedDescription=zero length data}

Jul 30 13:00:16 hostname sshd[1243]: Accepted password for usuario from
2001:db8:0:1::6 port 35849 ssh2
```

Registros de Eventos (*Logs*) – 2

Exemplos de *logs* de *firewall* pessoal:

```
#Software: Microsoft Windows Firewall

2005-04-11 08:05:57 DROP UDP 123.45.678.90 123.456.78.255 137 137 78 - - -
- - - - - RECEIVE

#Software: MacOS X Firewall

Jul 18 16:40:11 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:80 from 118.244.186.157:53031

Jul 18 16:46:22 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:8080 from 118.244.186.157:53031

Jul 18 16:49:30 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:3128 from 118.244.186.157:53031

Jul 18 16:59:09 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:22 from 116.10.191.176:6000

Jul 18 17:16:18 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:3389 from 218.77.79.43:47811

Jul 18 17:19:42 notebook Firewall[65]: Stealth Mode connection attempt to
TCP 192.0.2.209:22 from 116.10.191.223:6000

Jul 18 17:40:20 notebook Firewall[65]: Stealth Mode connection attempt to
UDP 192.0.2.209:5060 from 199.19.109.76:5079
```

Detecção de Atividades Maliciosas

IDS (*Intrusion Detection System*) – programa, ou um conjunto de programas, cuja função é detectar atividades maliciosas ou anômalas

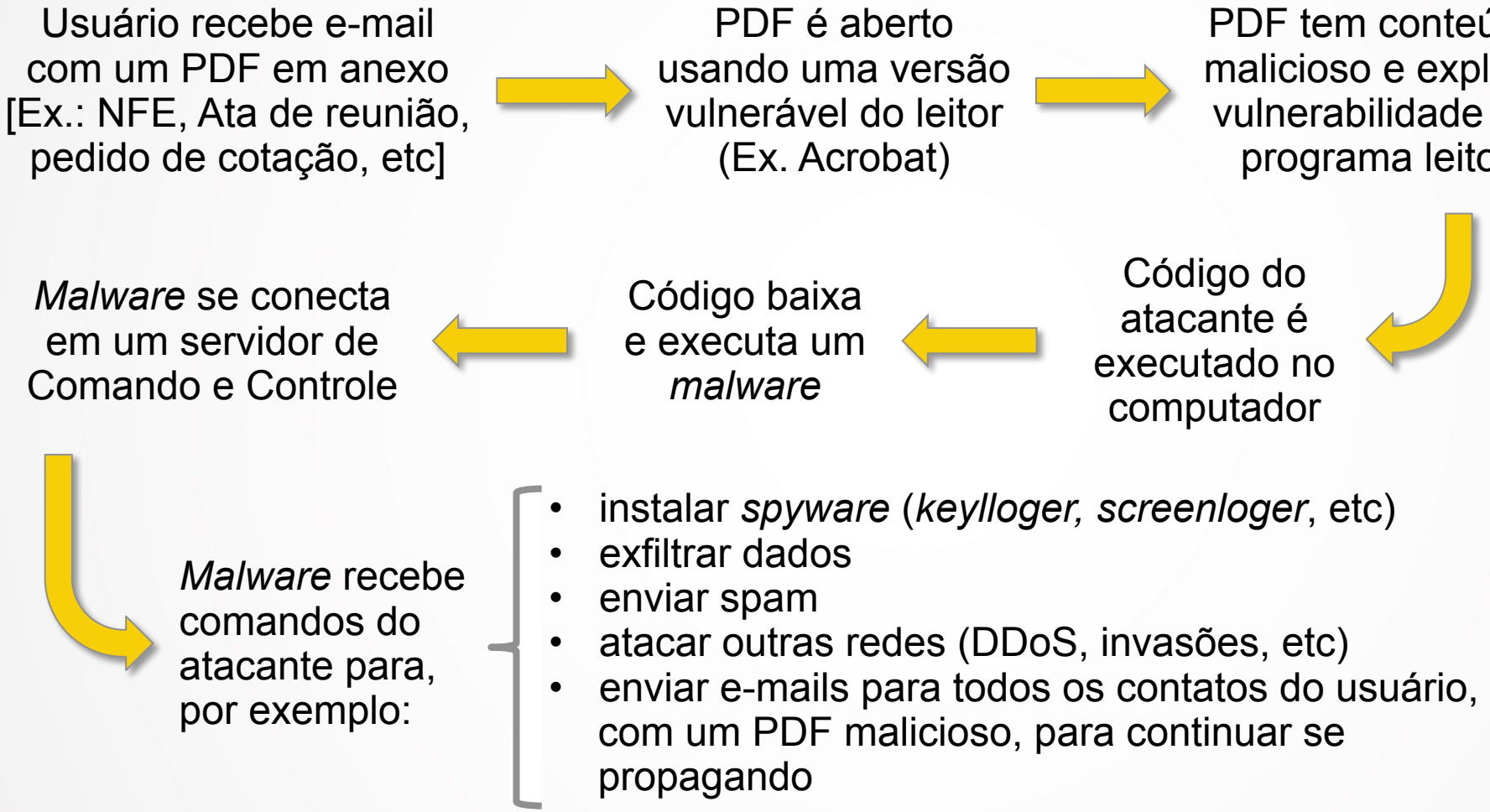
- geralmente implementado com base na análise de *logs* ou de tráfego de rede, em busca de padrões de ataque pré-definidos.

Fluxos de rede (*Flows*) – sumarização de tráfego de rede

- armazena IPs, portas e volume de tráfego
- permite identificar anomalias e perfil de uso da rede
- em segurança usado para identificar:
  - ataques de negação de serviço
  - identificar computadores comprometidos

Cenários Comuns de Ataques

Cenário:
Ataque Contra Usuários de Internet



Cenário:
Ataque Contra Servidores Web

Atacante instala ferramentas em um *site* já comprometido

Varre a Internet em busca de *sites* com sistemas CMS (Wordpress, Joomla, etc)

Constrói uma lista de *sites* a serem atacados

Em cada *site* realiza um ataque de força bruta de *logins* e senhas

Ao conseguir acesso ao *site* pode, entre outras coisas:

- alterar o seu conteúdo (*defacement*)
- desferir ataques contra outros sistemas ou redes (como DDoS, enviar *spam*, tentar invadir outros sistemas, etc)
- levantar páginas de *phishing*
- inserir *scripts* maliciosos, que são executados pelos navegadores dos visitantes (para infectar os usuários, alterar configurações do modem/wi-fi, etc)
- instalar suas ferramentas e iniciar a busca por outros *sites* com CMS para reiniciar o ciclo do ataque

Resiliência

Resiliência

Um sistema 100% seguro é muito difícil de atingir

Novo paradigma: 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

Gestão de Incidentes e Correlatos

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

Gestão de Incidentes – definição de políticas e processos que permitam a identificação e o tratamento de incidentes de segurança

CSIRT – acrônimo internacional para designar um Grupo de Resposta a Incidentes de Segurança, uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores

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

Inserção nas discussões de Governança:

IGF Best Practices Forums

- Establishing and supporting CSIRTs for Internet security
  http://www.intgovforum.org/cms/best-practice-forums/2-establishing-and-supporting-csirts
- Regulation and mitigation of unwanted communications (e.g. "spam")
  http://www.intgovforum.org/cms/best-practice-forums/regulation-and-mitigation-of-unwanted-communications

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 um investigador

Evolução histórica:
Tratamento de Incidentes no Brasil

Agosto/1996: o relatório "Rumo à Criação de uma Coordenadoria de Seguraça 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

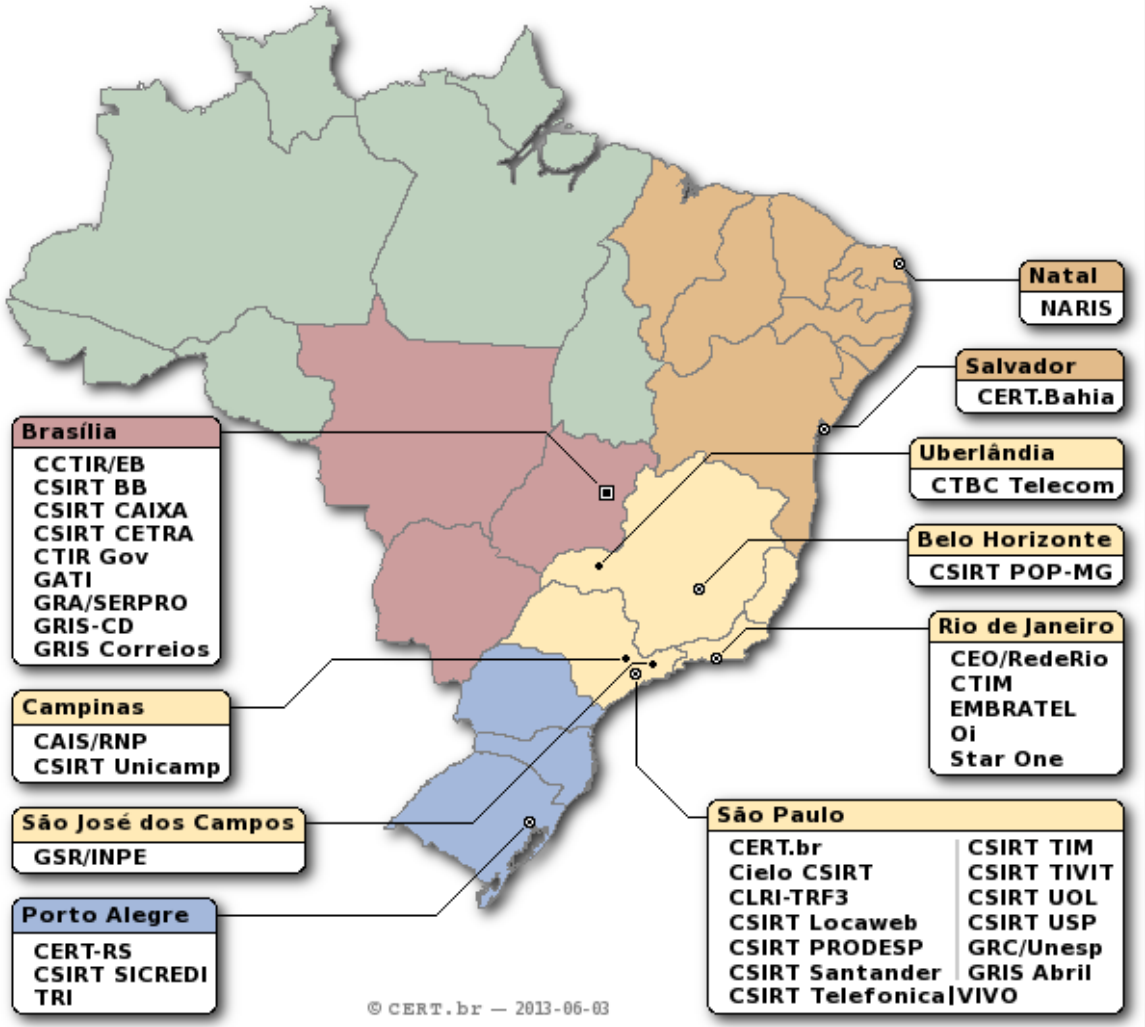
2002–2004 : grupos de trabalho para definição da estrutura de um CSIRT para a Administração Pública Federal

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: **37 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, GRA/SERPRO, 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	CSIRT TIVIT, GRIS Abril



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

Fóruns Internacionais de Segurança

FIRST – *Forum of Incident Response and Security Teams*

- **Criação:** 1990
- **Membros:** 326 CSIRTs, de mais de 70 países, participantes de todos os setores;

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*"

Colocando em Prática os Príncipios de Governança

CGI.br/RES/2009/003/P - PRINCÍPIOS PARA A GOVERNANÇA E USO DA INTERNET NO BRASIL - Fevereiro de 2009

8. Funcionalidade, segurança e estabilidade
A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de **medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas**.

NETmundial Multistakeholder Statement - April, 24th 2014, 19:31 BRT

SECURITY, STABILITY AND RESILIENCE OF THE INTERNET

Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. **Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders.**

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

Boas práticas para reduzir o "poder de fogo":

- **Detentores de ASN:** 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 código mais seguro

Prevenção por parte das vítimas:

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

Repressão por parte das polícias:

- Investigar e punir os atacantes

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

Quem tem acesso? Com que finalidade?

Como estes dados estão protegidos?

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

Privacidade *online*

Um grande risco pode ser não entender a tecnologia

- As informações que um navegador fornece a um *site*, permitem identificação mais únivoca que um endereço IP válido
- Medidas de segurança não são contra a privacidade, mas sim essenciais para mantê-la

É necessário que modelos de negócio e regras sejam claros

- Serviços não são gratuitos, são pagos com informações providas por seus usuários

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* (cripto 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.

Hospira Plum A+ and Symbiq Infusion Systems Vulnerabilities | ICS-CERT

https ics-cert.us-cert.gov/advisories/ICSA-15-161-01 Reader

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.

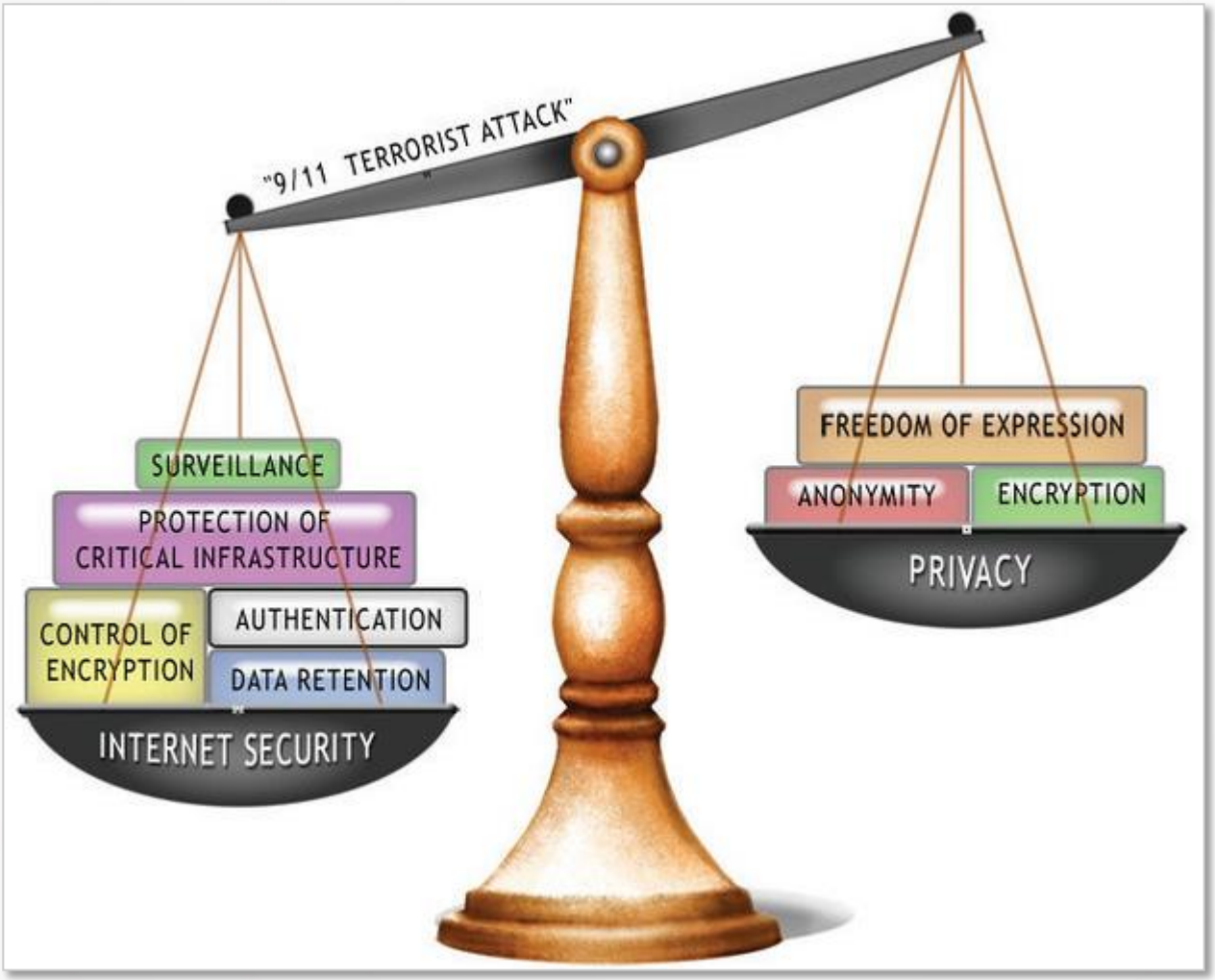
CVE-2015-3954[f] has been assigned to this vulnerability. A CVSS v2 base score of 10.0 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[g]

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.

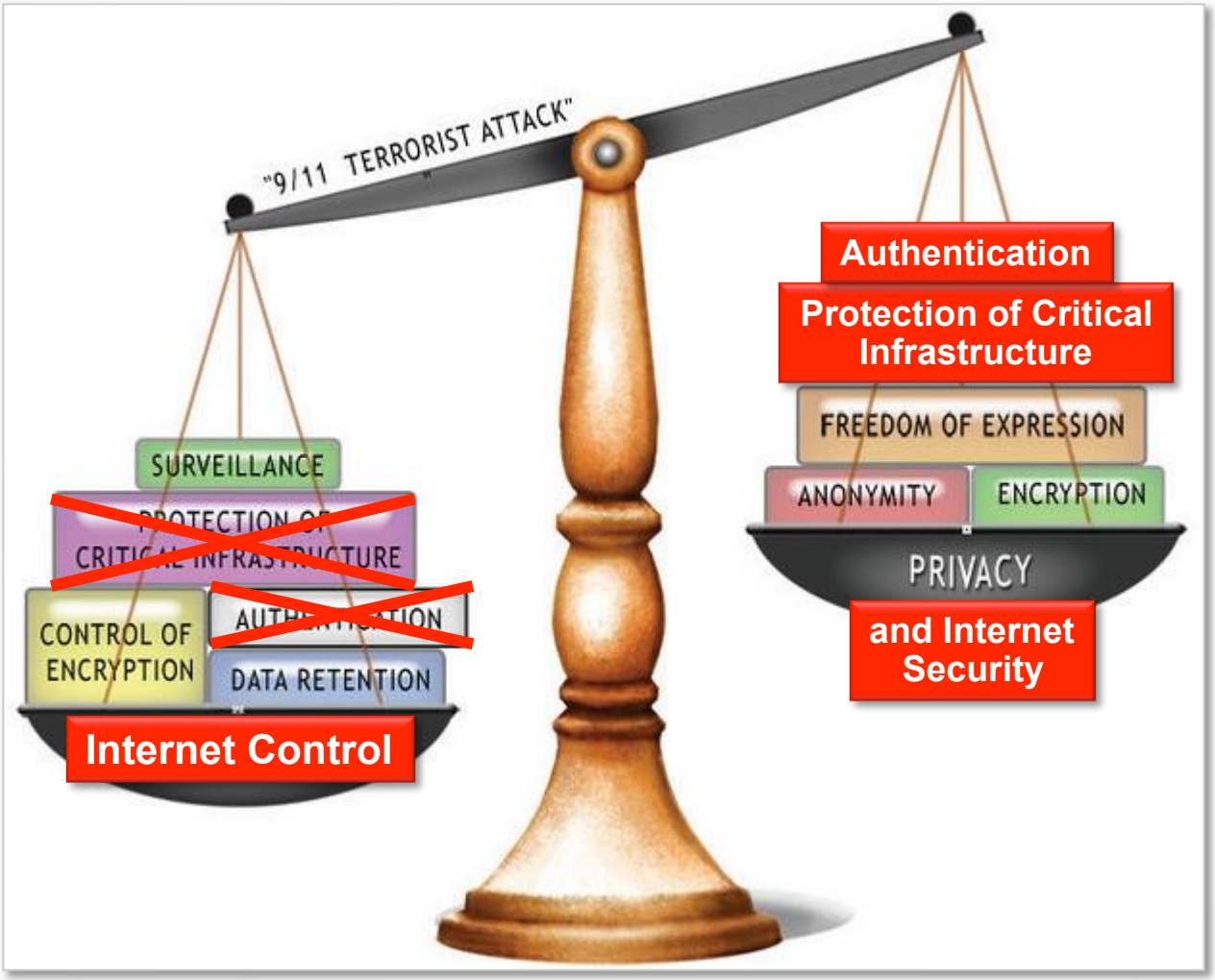
Fato ou Mito?

Diplo Foundation:
Security vs. Privacy



Fonte:
http://pt.slideshare.net/DiploFoundation/gic-introduction-to-ig

Como poderia ser uma balança 2.0:
~~Security~~Control vs. Privacy and Security



Fonte:
http://pt.slideshare.net/DiploFoundation/gic-introduction-to-ig

Fato ou Mito?

“Para implementar Gerência de Porta 25 é preciso olhar o conteúdo dos pacotes”

Fato ou Mito?

“*Logs* são necessários para conseguir segurança e privacidade”

Fato ou Mito?

“Para evitar vigilância (*surveillance*) a solução é cifrar todas as comunicações, protocolos e acessos na Internet”

Fato ou Mito?

“Para proteger é necessário saber invadir”

Referências:
Fontes dos Conceitos Apresentados

Cartilha de Segurança para a Internet
http://cartilha.cert.br/

Security Engineering, 2nd Edition, 2008, Ross Anderson
http://www.cl.cam.ac.uk/~rja14/book.html

Glossary of Security Terms,* SANS *Institute
http://www.sans.org/security-resources/glossary-of-terms/

RFC 2196: Site Security Handbook
http://tools.ietf.org/html/rfc2196

Cyber Risk and Resilience Management, CERT/CC
http://www.cert.org/resilience/

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