
egi
Escola de Governança
da Internet no Brasil

Ecossistema da Segurança Cibernética

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

09/07/2018

MOTHERBOARD

How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet

As many predicted, hackers are starting to use your Internet of Things to launch cyberattacks.

Officials: DC security cameras hacked 8 days before inauguration by man, woman in London

by John Gonzalez/ABC7 | Friday, February 3rd 2017

Hacking intelligent buildings using KNX and Zigbee networks

A great many of us are living, staying or working in "smart" buildings, relying on automated processes to control things like heating, ventilation, air conditioning, lighting, security and other operation systems. We expect those systems to work without a glitch and withstand attacks but, unfortunately, the security of these systems is still far from perfect.

Network live IP video cameras directory Insecam.com

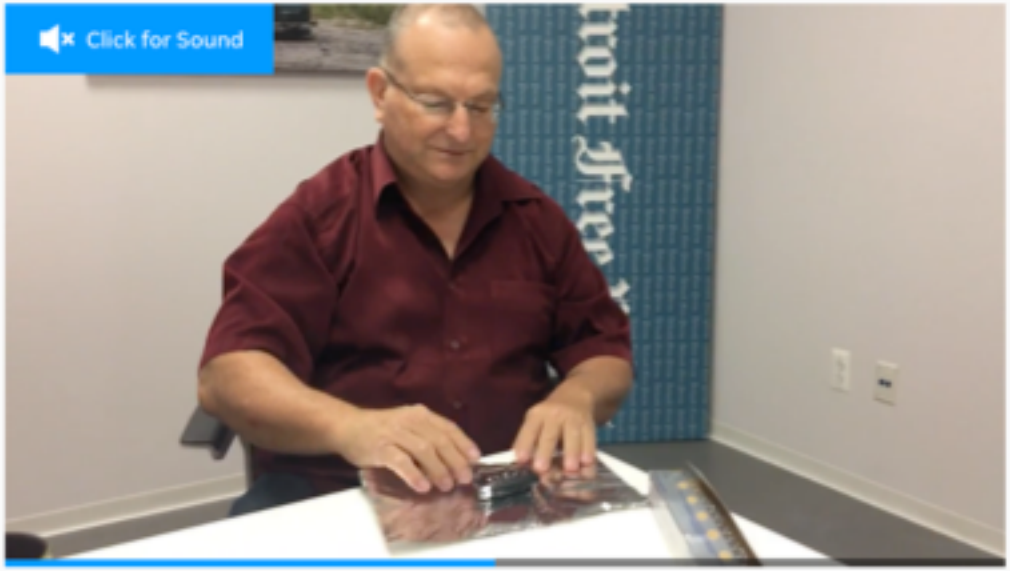
Welcome to Insecam project. The world biggest directory of online surveillance security cameras. Select a country to watch live street, traffic, parking, office, road, beach, earth online webcams. Now you can search live web cams around the world. You can find here Axis, Panasonic, Linksys, Sony, TPLink, Foscam and a lot of other network video cams available online without a password. Mozilla

USA TODAY NEWS SPORTS LIFE MONEY TECH TRAVEL OPINION 63° SUBSCRIBE MORE

BREAKING NEWS Fifth boy reportedly rescued from Thai cave as perilous rescue effort continues; watch livestream Read Story

Why you might want to wrap your car key fob in foil

USA TODAY NETWORK Phoebe Wall Howard, Detroit Free Press Published 6:00 a.m. ET July 8, 2018



How to keep your car's key fob safe. Phoebe Wall Howard, Detroit Free Press

Objetivos

Discutir os conceitos técnicos relacionados com segurança, privacidade e resiliência e o ecossistema de segurança cibernética

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 da Informação e Segurança da Internet

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.

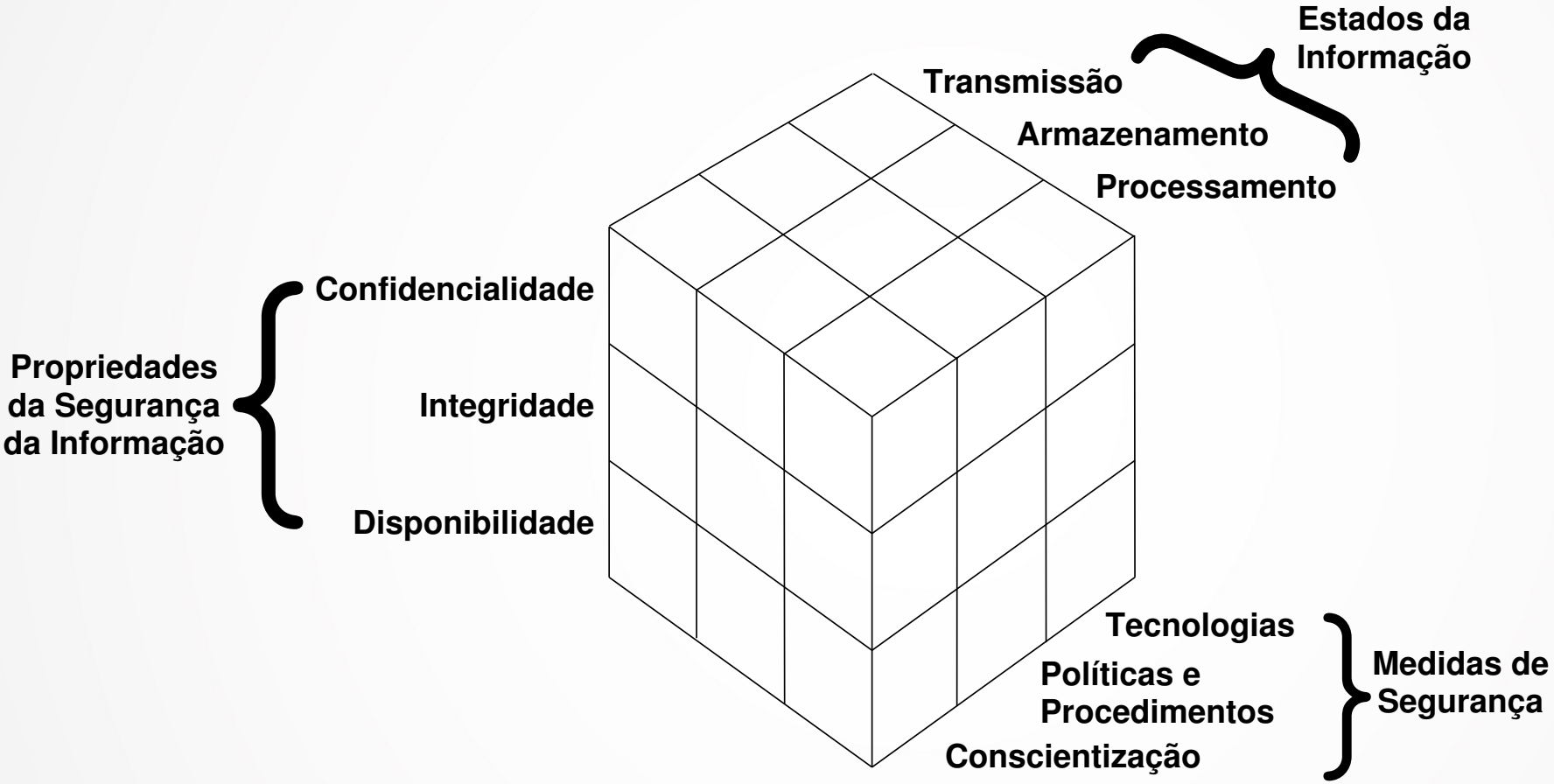
Ex. de quebra: alguém obtém acesso não autorizado ao seu computador e altera informações da sua declaração de Imposto de Renda, momentos antes de você enviá-la à Receita Federal.

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.

egi

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/

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

Características da Internet

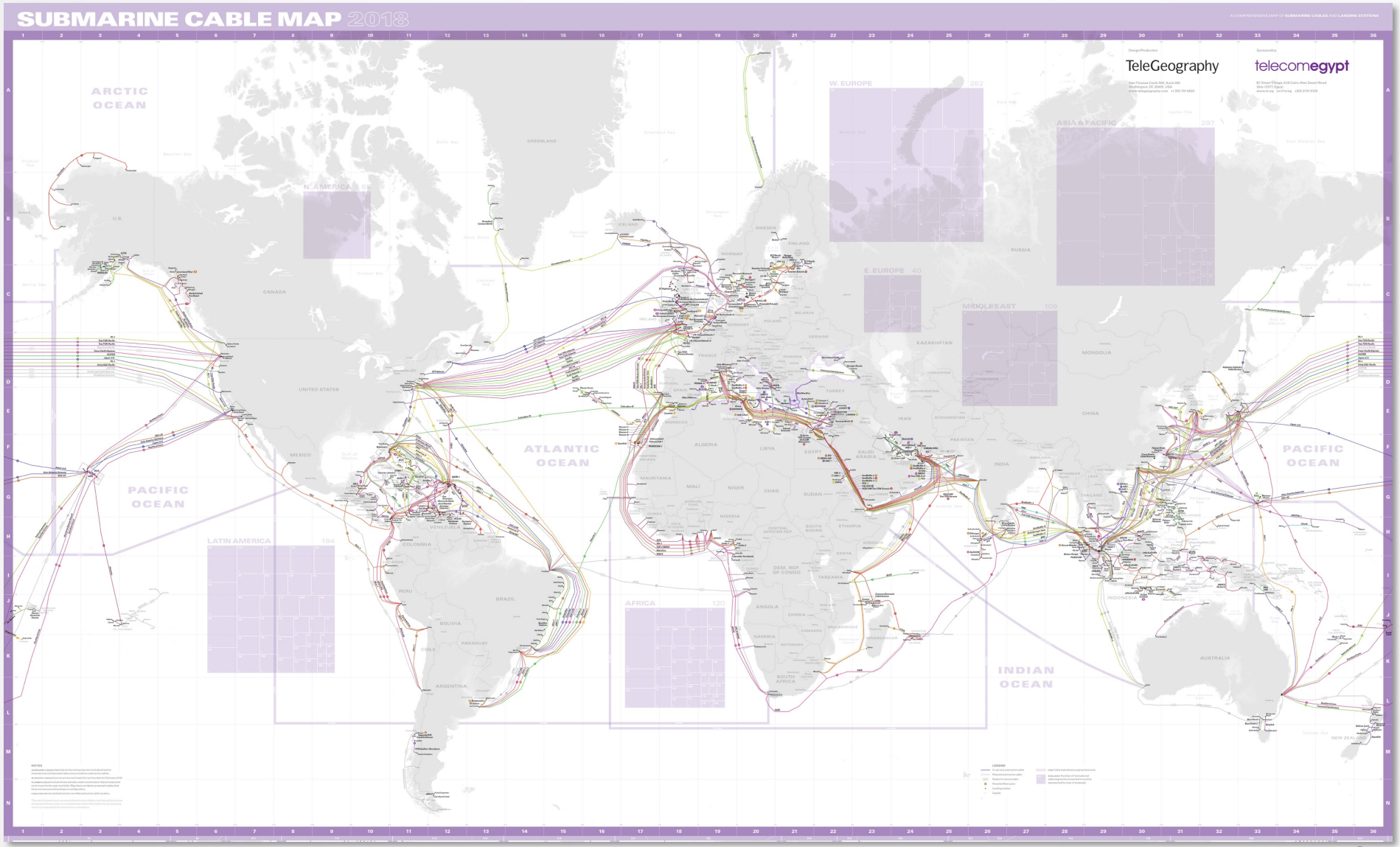
"Rede de redes"

- Sistema de redes interconectadas
- Sem controle centralizado
  - Redes independentes e autônomas entre si
- Rede global
  - Atualmente mais de 50 mil "sistemas autônomos" (número de redes maior que isso)

Sistemas Autônomos

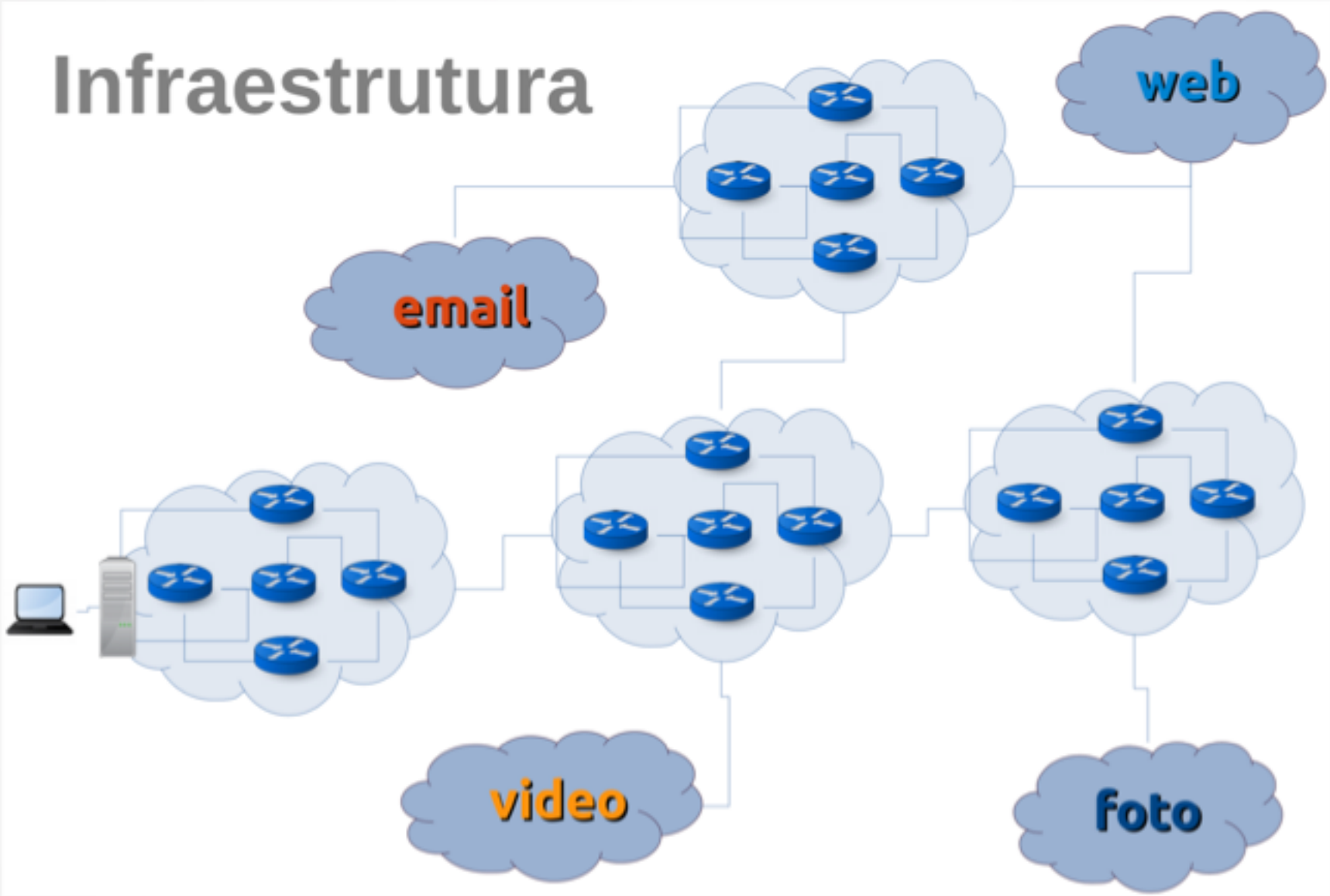
- Conjunto de equipamentos sob uma mesma administração e com políticas de roteamento próprias
- **Autonomia** em relação aos demais sistemas/redes
- Identificação única:
  - ASN (*Autonomous System Number*)

Internet

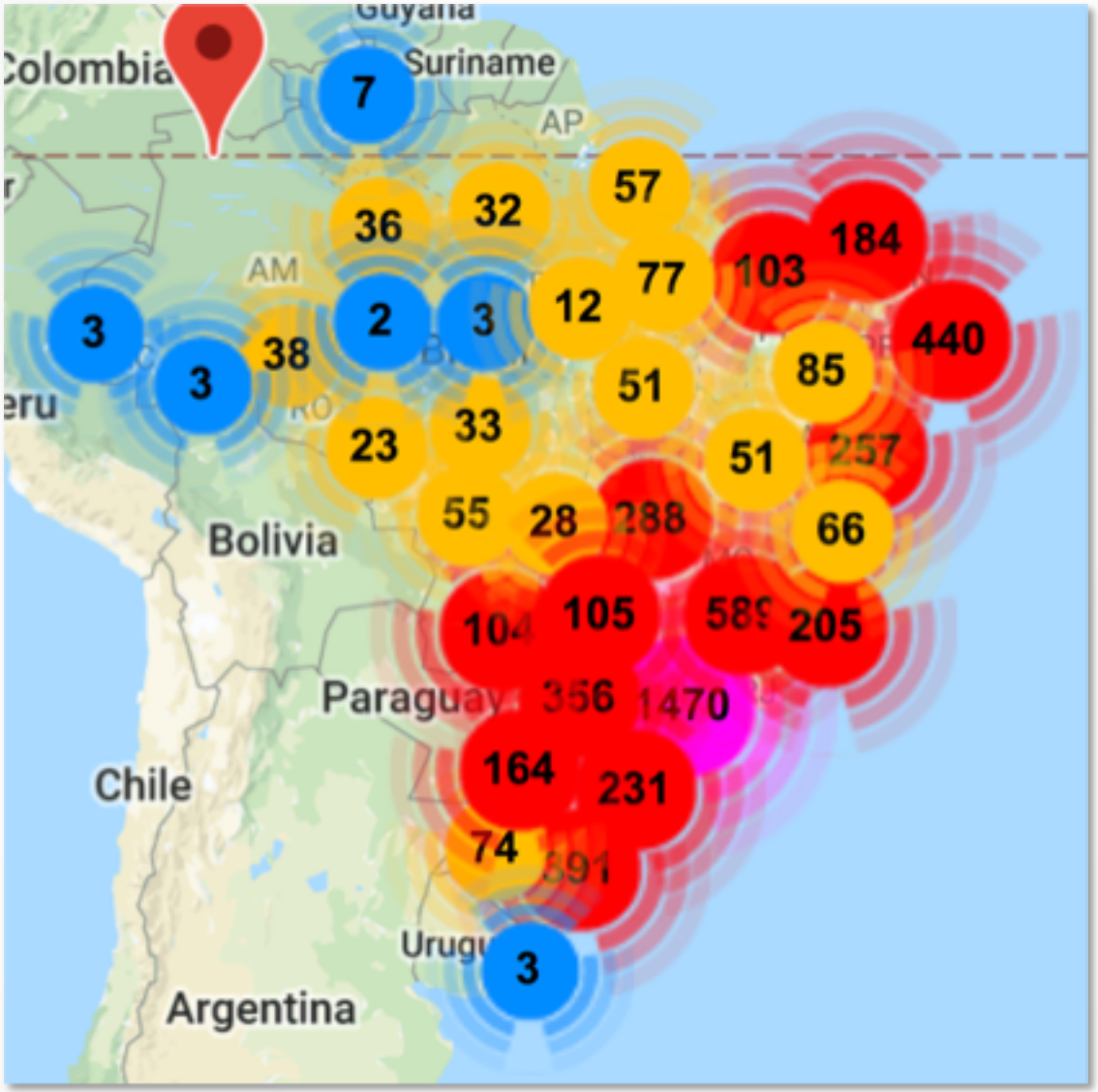


Fonte: https://www2.telegeography.com/submarine-cable-map

Internet e Sistemas Autônomos



Sistemas Autônomos no Brasil: 5627



http://ix.br/localidades/brasmap

Resiliência das Organizações:
Resistir e Continuar Operando sob Ataques

Objetivo primordial é um ecossistema saudável

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

Administradores de redes e sistemas

- não emanar “sujeira” de suas redes e adotar boas práticas

Usuários

- entender os riscos e seguir as dicas de segurança
- manter seus dispositivos atualizados e tratar infecções

Desenvolvedores

- precisam pensar em segurança desde as etapas iniciais de desenvolvimento

Ainda assim incidentes ocorrerão

- **necessário identificar e mitigar mais rapidamente**
- **é necessário ter CSIRTs estabelecidos e profissionais preparados**

CSIRT: Grupo de Tratamento de Incidentes de Segurança em Computadores, do Inglês *Computer Security Incident Response Team*

egi

Resiliência das Organizações:
Papel dos CSIRTs na Mitigação e Recuperação

Tratamento de Incidentes é só um de vários processos essenciais

- Gestão de Risco, Segurança da Informação, Continuidade de Negócios, Segurança de Desenvolvimento, Gestão de Atualizações e de Configuração

A redução do impacto de um incidente é conseqüência da

- agilidade de resposta
- redução no número de vítimas

O sucesso depende da confiança (trust)

- nunca divulgar dados sensíveis nem expor vítimas, por exemplo

O papel de um CSIRT é

- auxiliar a proteção da infraestrutura e das informações
- prevenir incidentes e conscientizar sobre os problemas

O CSIRT não é um investigador

- A decisão de levar um caso à justiça deve ser da vítima
- Em uma organização, leia-se: alta administração e setor jurídico

Cooperação é primordial – nacional e internacional

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

SEI Partner Carnegie Mellon

FIRST Improving Security Together MEMBER

APWG RESEARCH PARTNER www.antiphishing.org

The Honeynet PROJECT

Principais atividades:

Tratamento de Incidentes

- Ponto de contato nacional para notificação de incidentes
- Atua facilitando o processo de resposta a incidentes das várias organizações
- Trabalha em colaboração com outras entidades
- Auxilia novos CSIRTs a estabelecerem suas atividades

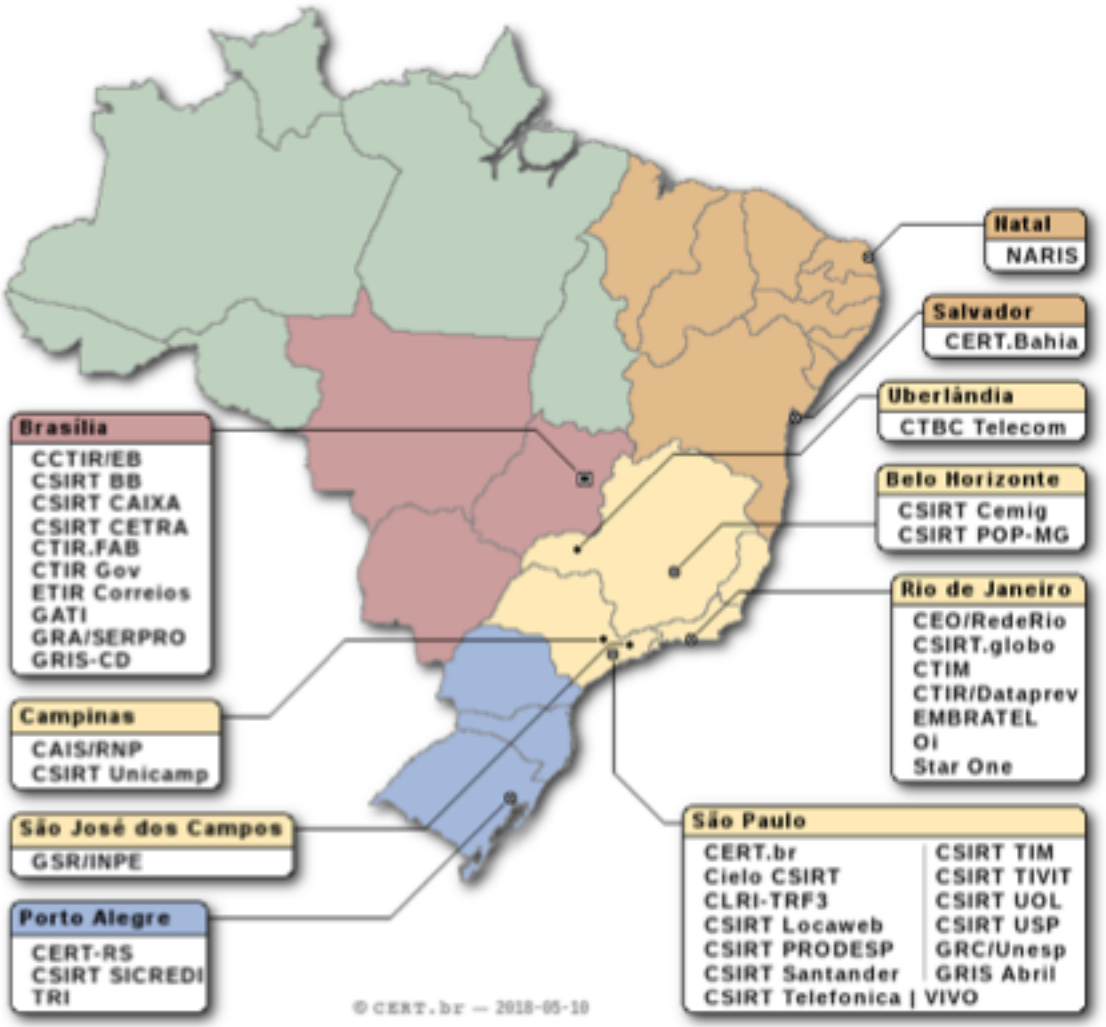
Formação de profissionais para atuar em Tratamento de Incidentes

Produção de boas práticas e material para conscientização sobre a necessidade de segurança na Internet para diversas audiências

egi

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

Setor	CSIRTs
Nacional – domínios .br, ASNs ou IPs alocados ao Brasil.	CERT.br
Nacional – Administração Pública Federal	CTIR Gov
Governo	CCTIR/EB, CLRI-TRF-3, CSIRT CETRA, CSIRT PRODESP, CTIM, CTIR.FAB, CTIR/Dataprev, ETIR Correios, GATI, GRA/SERPRO, GRIS-CD
Energia	CSIRT Cemig
Sistema Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Santander, CSIRT Sicredi
Provedores Operadoras Hospedagem	CSIRT Locaweb, CSIRT TIM, CSIRT TIVIT, CSIRT UOL, CSIRT Telefonica|VIVO, CTBC Telecom, EMBRATEL, StarOne, Oi
Academia	CAIS/RNP, CEO/RedeRio, CERT-RS, CERT.Bahia, CSIRT POP-MG, CSIRT Unicamp, CSIRT USP, GSR/INPE, GRC/UNESP, NARIS, TRI
Outros	CSIRT.globo, GRIS Abril



https://cert.br/csirts/brasil/

Fóruns Internacionais de Segurança e Combate a Abusos na Internet

FIRST – *Forum of Incident Response and Security Teams*

- **Criação:** 1990
- **Membros:** 429 CSIRTs, de 89 países, participantes de todos os setores;

APWG – (originalmente *AntiPhishing Working Group*)

- **Criação:** 2003
- **Membros:** mais de 2.000 organizações, participantes de todos os setores, incluindo organizações internacionais;

M^{3}AAWG – *Messaging, Mobile, Malware Anti-Abuse Working Group*

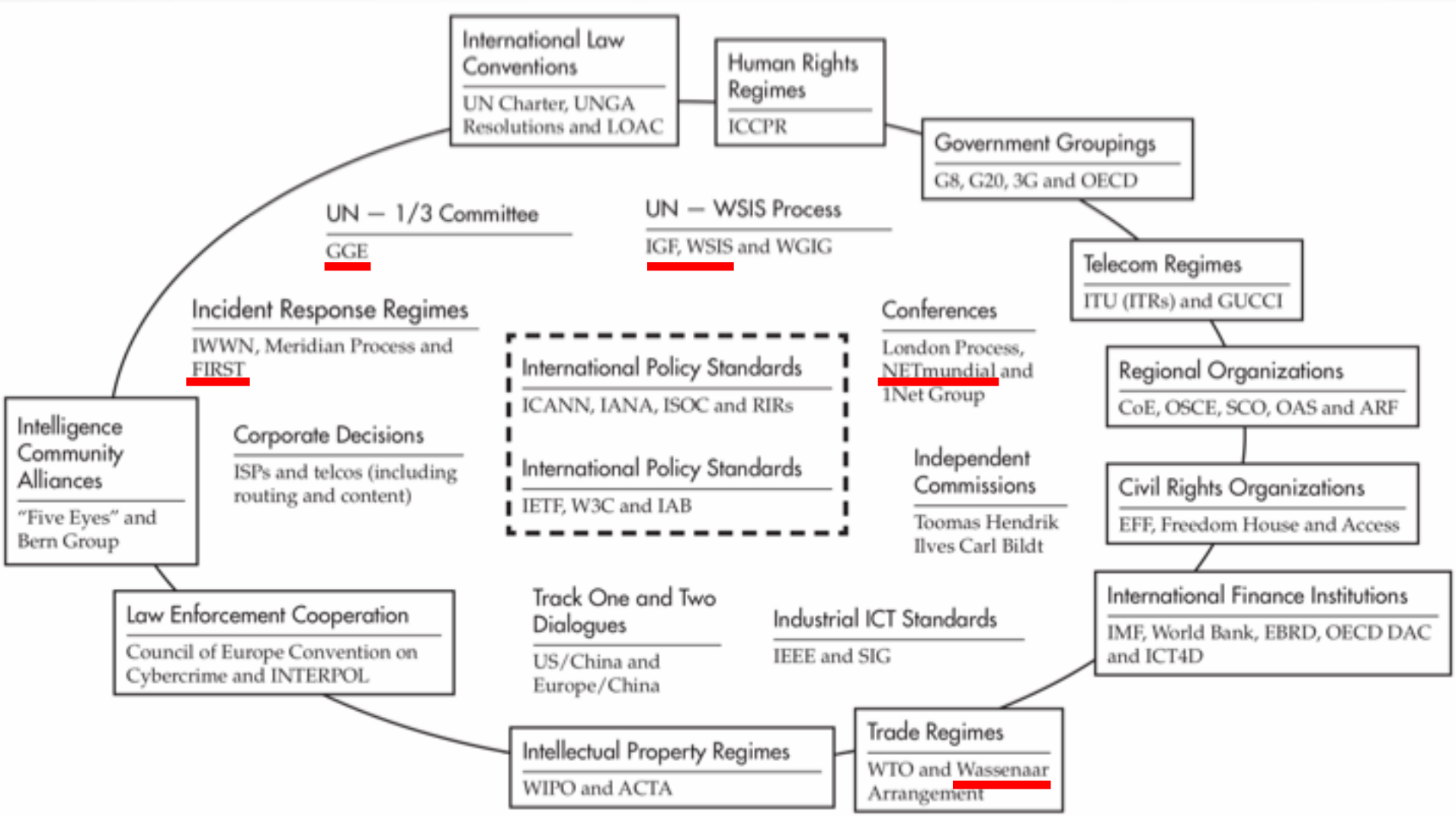
- **Criação:** 2004
- **Membros:** mais e 200 membros da Indústria – "*Internet Service Providers (ISPs), telecomm companies, Email Service Providers (ESP), social networking companies, leading hardware and software vendors, major brands, major antivirus vendors and numerous security vendors*"

LAC-AAWG – *Latin American and Caribbean Anti-Abuse Working Group*

- **Criação:** 2017
- **Membros:** Comunidade Internet em Geral; mantido pelo LACNOG, LACNIC e M^{3}AAWG.

Segurança e Governança da Internet

egi



The Regime Complex for Managing Global Cyber Activities
Global Commission on Internet Governance Paper Series No. 1
May 20, 2014, Joseph S. Nye Jr.
https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

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://netmundial.br/netmundial-multistakeholder-statement/

UN GGE

UNODA
UNITED NATIONS OFFICE FOR DISARMAMENT AFFAIRS

UN General Assembly, Group of Governmental Experts, Document A/70/174
22 July 2015

[...]

States should not conduct or knowingly support activity to **harm the information systems of the authorized emergency response teams** (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

[...]

https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies – December 2017

4. E. 1. "Technology" as follows:

a. "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D.

[...]

c. "Technology" for the "development" of "intrusion software".

Note 1 **4.E.1.a. and 4.E.1.c. do not apply to 'vulnerability disclosure' or 'cyber incident response'.**

Note 2 Note 1 does not diminish national authorities' rights to ascertain compliance with 4.E.1.a. and 4.E.1.c.

Technical Notes

1. **'Vulnerability disclosure' means** the process of identifying, reporting, or communicating a vulnerability to, or analysing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.
2. **'Cyber incident response' means** the process of exchanging necessary information on a cyber security incident with individuals or organizations responsible for conducting or coordinating remediation to address the cyber security incident.

[...]

https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf

"*0-Days*" e Governos Estocando Vulnerabilidades: **Do *EternalBlue* ao *WannaCry***

2012 (ou antes) – NSA descobre uma vulnerabilidade grave nos sistemas Windows, que permite comprometimento remoto. Dá o nome de *EternalBlue* e não divulga a ninguém.

1º Semestre de 2016 – um grupo chamado *The Shadow Brokers* ganha acesso a dados da NSA, que incluem diversas vulnerabilidades, entre elas o *EternalBlue*.

Agosto de 2016 – *The Shadow Brokers* começa a colocar publicamente na Internet algumas das ferramentas da NSA.

07 de janeiro de 2017 – *The Shadow Brokers* começa a vender algumas das ferramentas, incluindo o *EternalBlue*.

Janeiro/Fevereiro de 2017 – NSA contata a Microsoft com detalhes sobre a vulnerabilidade.

14 de março de 2017 – Microsoft lança a correção MS17-010, que corrige a vulnerabilidade identificada como CVE-2017-0144 – o *EternalBlue*.

14 de abril de 2017 – O grupo *The Shadow Brokers* dilvulga 300MB de materiais da NSA no Github, incluindo o *EternalBlue*.

12 de maio de 2017 – Tem início a propagação do *Ransomware WannaCry*.

https://boot13.com/windows/timeline-nsa-hacking-tool-to-wannacry/

https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Questões Persistentes em Fóruns Globais

Debate:
Segurança vs. Privacidade

"*Para ter segurança é preciso abrir mão da privacidade*"

"*Na Internet, não se deve analisar nem os cabeçalhos dos pacotes*"

"*Órgãos investigativos precisam ter acesso a comunicações criptografadas para serem efetivos*"

"*Para ter privacidade deve-se eliminar*
- *logs*
- *cookies*"

"*Usar criptografia em todas as comunicações garante privacidade*"

Considerações:
Controle vs. Segurança vs. Privacidade

Medidas de Segurança

- criptografia
- controle de acesso
  - garantir que só você acessa sua conta de *e-mail*; que ninguém invade seu perfil do *twitter,* etc
  - garantir que só você acessa seu *Internet banking*
- amazenar *logs* de acordo com políticas bem definidas e para fins específicos de segurança e funcionamento da rede

Medidas de Controle

- armazenar 100% do tráfego
- armazenar, inspecionar e processar de forma centralizada *logs*, consultas DNS, acessos, conteúdo, etc
  - de múltiplas redes
  - correlacionando estas informações
  - com motivações diversas e difusas

Considerações:
Privacidade *Online*

Um grande risco à privacidade pode ser simplesmente 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

DPI é um *buzzword* criado pela indústria para vender "caixas"

- Sem "olhar" os cabeçalhos e os IPs, os pacotes não chegam ao destino
- Antivírus, *antispam*, IDS e alguns *firewalls* necessitam inspecionar o "conteúdo" à busca de assinaturas de ataques
- O importante é isto ocorrer com políticas bem definidas e para fins específicos de segurança ou funcionamento da rede

Considerações:
Leitura Complementar Recomendada

Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications

http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

"*This report's analysis of law enforcement demands for exceptional access to private communications and data shows that* ***such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend***."

Ataques DDoS usando dispositivos IoT

Atacantes exploram senhas fracas ou padrão

Foco em dispositivos com versões "enxutas" de Linux

- para sistemas embarcados
- arquiteturas ARM, MIPS, PowerPC
- exemplos: CCTV, DVR, CPEs (*Consumer Premises Equipments,* como modems banda larga, rotadores wi-fi), Discos Externos, etc.

Malware* se instala e conecta no comando e controle de uma *botnet

Atacante envia comandos

- alvo do ataque
- tipo do ataque (TCP, UDP, grande volume, grande número de conexões, etc)

Referências para Acompanhar as Discussões Globais

IGF Best Practices Forums

- **Relatórios finais das discussões dos fóruns sobre "*Establishing and supporting CSIRTs*" e "*Fighting Spam*"**

  2015: http://www.intgovforum.org/cms/best-practice-forums/2015-best-practice-forum-outputs

  2014: http://www.intgovforum.org/cms/best-practice-forums/igf-2014-best-practices-forums

- **Fórum ativo no IGF é o "*Best Practices Forum on Cybersecurity*". O foco deste ano é: "*culture, norms and values in cybersecurity*"**

  2016–2018: https://www.intgovforum.org/multilingual/content/bpf-cybersecurity-1

FIRST Internet Governance Initiative

https://first.org/global/governance/

FIRST Incident Handling for Policy Makers

https://first.org/education/incident_handling_for_policy_makers/Incident_Response_for_Policymakers_v1.2.1.pptx.zip

Referências para Acompanhar as Discussões Globais (cont.)

Cadernos CGI.br

https://www.cgi.br/publicacoes/indice/livros/

- **Combate ao spam na Internet no Brasil: Histórico e reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil**
  https://www.cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil-historico-e-reflexoes-sobre-o-combate-ao-spam-e-a-gerencia-da-porta-25-coordenados-pelo-comite-gestor-da-internet-no-brasil/

- **Declaração Multissetorial do NETmundial**
  https://www.cgi.br/publicacao/cadernos-cgi-br-declaracao-multissetorial-do-netmundial/

- **Documentos da Cúpula Mundial sobre a Sociedade da Informação: Genebra 2003 e Túnis 2005**
  https://www.cgi.br/publicacao/cadernos-cgi-br-documentos-cmsi/

Colocando em Prática os Princípios de Governança Colaborativa para Segurança na Internet

egi

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.

Atores 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 (*hardening*), "limpar" dispositivos infectados
- **Desenvolvedores de sistemas:** considerar riscos no projeto, desenvolver código mais seguro, configuração padrão mais segura
- **Academia:** formar profissionais de todas as áreas que considerem segurança como essencial

Prevenção por parte das vítimas:

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

Repressão por parte dos operadores da justiça:

- Investigar e punir os atacantes

Boas Práticas Operacionais para Sistemas Autônomos: **Ações da Comunidade para Melhorar a Internet**

Boas práticas para aumentar a resiliência e estabilidade das redes:

- Segurança de roteamento
- *Antispoofing*
- Redução e mitigação de DDoS

Parte da Iniciativa "*Por uma Internet mais Segura*"

Lançamento conjunto na Semana de Infraestrutura da Internet no Brasil por

- Abranet
- Abrint
- ISOC
- NIC.br
- SindiTelebrasil

Trabalho de organizações internacionais:

- ISOC – MANRS.org
- IETF – BCP 38 (*antispoofing*)
- M^{3}AAWG, LAC-AAWG, LACNOG and LACNIC: BCOP para compra e especificação de CPEs

https://bcp.nic.br/

https://nic.br/noticia/releases/programa-para-fazermos-uma-internet-mais-segura-sera-lancado-na-vii-semana-de-infraestrutura/

Obrigado

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

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

20 anos cert.br

nic.br cgi.br

www.nic.br | www.cgi.br