nic.br cgi.br | cert.br

7º Fórum Brasileiro de CSIRTs

São Paulo, SP | 14 de setembro de 2018

ONU, OTAN, ITU, GCSC, GCCS, GFCE, Controle de Armamentos...

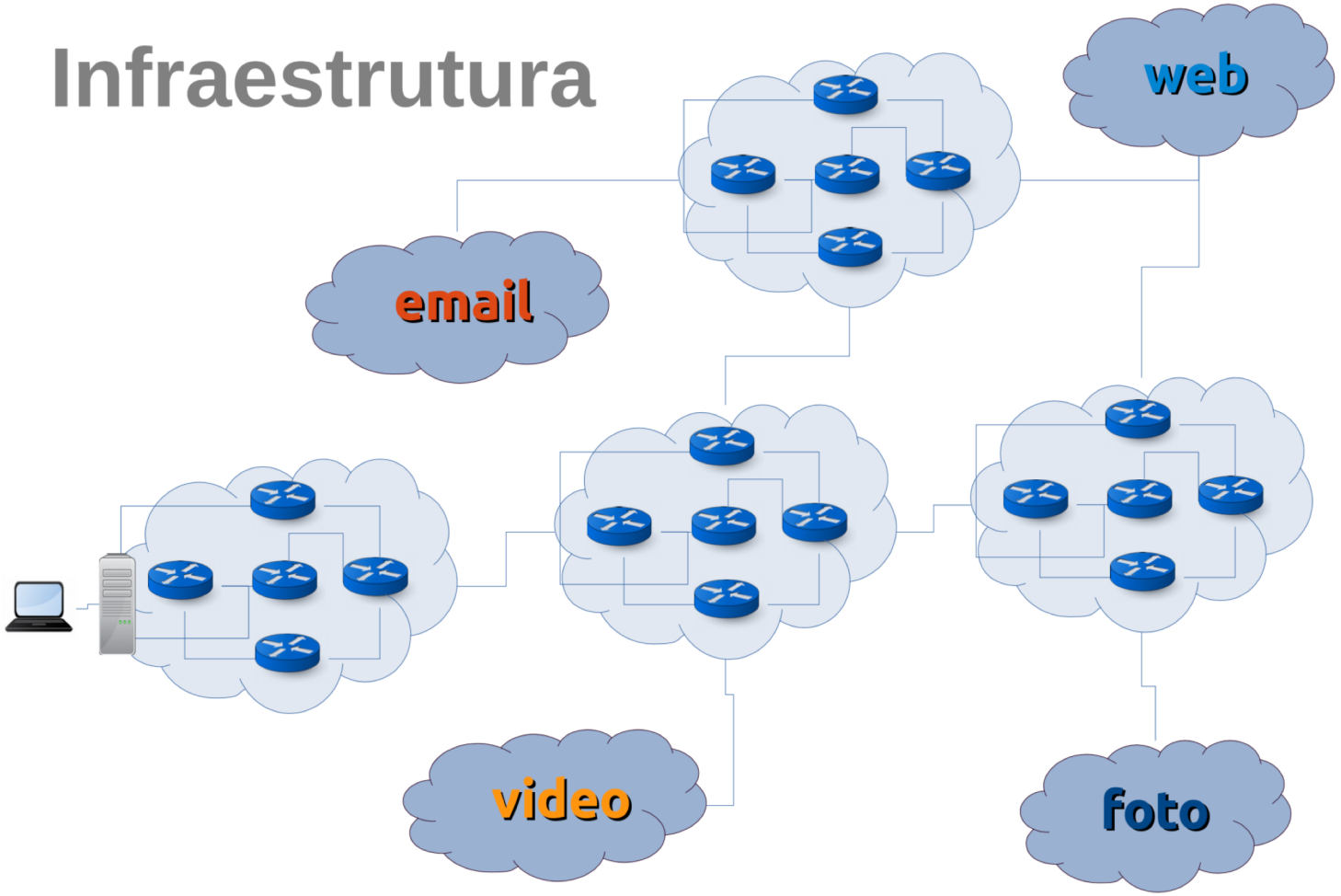
Como decisões políticas e normas globais podem afetar o trabalho dos CSIRTs, a sua segurança e a da Internet

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

cert.br nic.br cgi.br

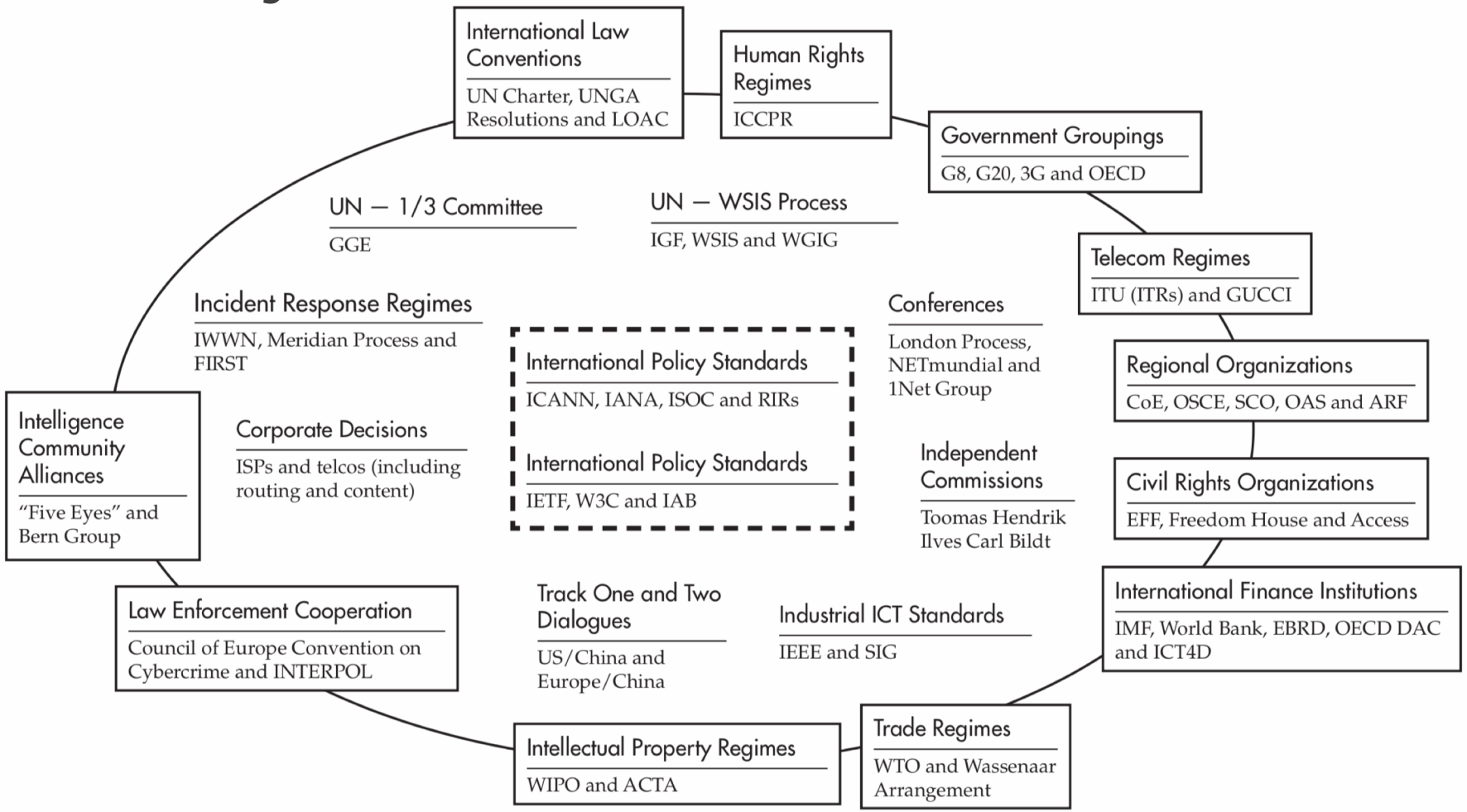
Atores envolvidos em decisões na Internet: **Visão da Comunidade Técnica**

- ASes / Provedores / Empresas
- Fabricantes de *Software* e *Hardware*
- Padrões (IETF, W3C, IEEE)
- *Compliance* (ISO, PCI, ABNT)
- ICANN / RIRs
- Gestores
- Jurídicos
- Ferramentas
  - *logs*, *appliances*, algoritmos e afins



Fonte: Fundamentos Técnicos – Arquitetura da Internet, Ricardo Patara
EGI Curso Jurídico, Rio de Janeiro, RJ, 21/11/2016

Atores envolvidos em decisões na Internet: **Visão dos "*Policy Makers*"**



Fonte: 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

Alguns dos Maiores Desafios

Técnicos

- A Internet realmente não tem fronteiras
- Ocultar a fonte dos ataques é muito fácil
- “Atribuição” é muito difícil
- Tanto sistemas críticos e sistemas de uso geral compartilham o mesmo *software*
  - todos os países usam o mesmo *software*
- Aumentar a segurança depende de as vulnerabilidades serem descobertas, conhecidas e corrigidas

Políticos

- As leis e normas são territoriais
- Governos historicamente não confiam uns nos outros
- Forças Militares e de Segurança Nacional aplicam a lógica da Guerra Fria e de Desarmamento para o cenário digital
  - “estocar armas” (aka vulnerabilidades)
  - impedir “inimigos” de ter ter acesso a estas “armas”

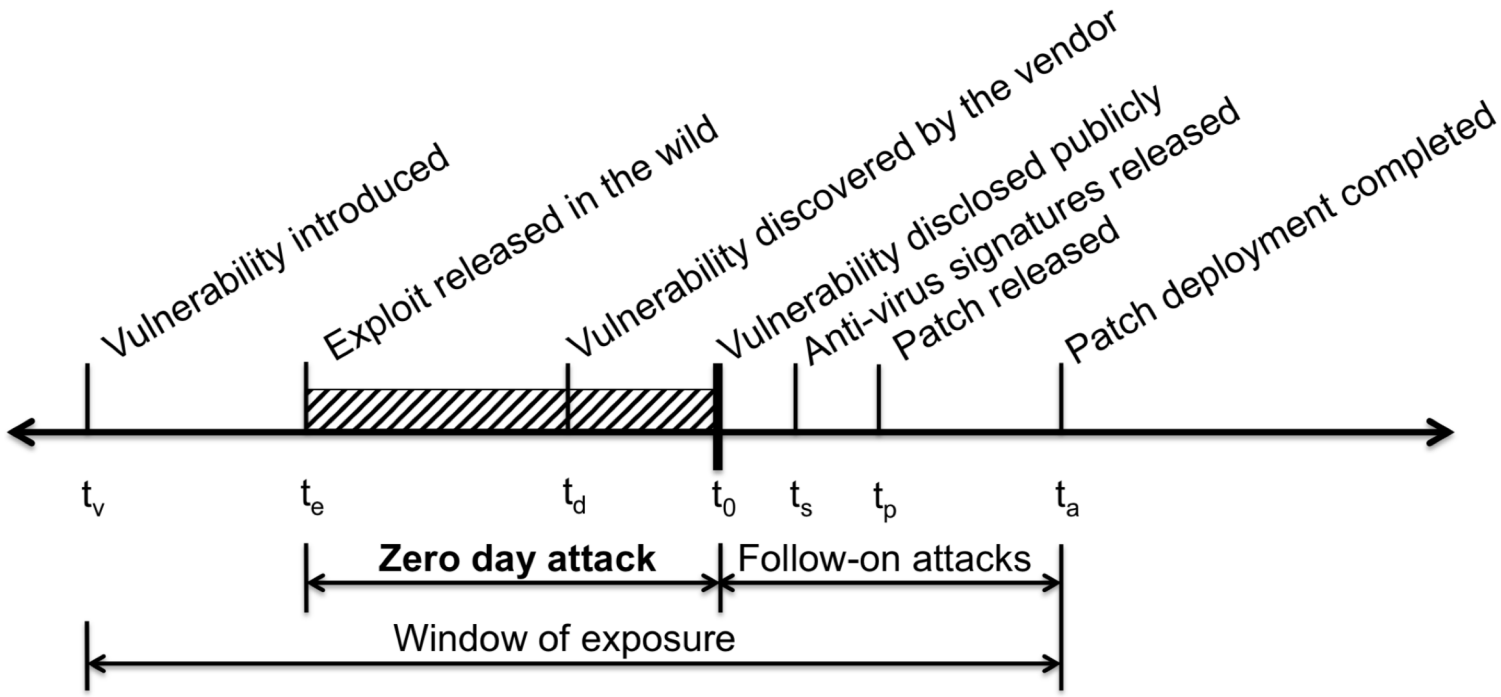
Conseguimos proteger nossos sistemas?
Responsible Disclosure vs. Stock Pilling Vulnerabilities

Desafios no cenário

- Vulnerabilidades descobertas pelos governos e mantidas em “segredo”
- Mercado de compra e venda de *zero days*
  - Governos são os principais compradores dos *brokers* legítimos
  - “Pesquisadores” tendem a vender para quem pagar mais
  - Programas de *Bug Bounty* dos fabricantes não conseguem competir

➢ Dura verdade: só há patches se o fabricante conhece a vulnerabilidade, fora isso, todos estamos vulneráveis

Attack Timeline



Fonte: ***Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World Proceedings of the 2012 ACM Conference on Computer and Communications Security***
http://doi.acm.org/10.1145/2382196.2382284

Onde estas questões estão sendo discutidas?

cert.br nic.br cgi.br

World Summit on the Information Society (WSIS - ONU): **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

Governança de Internet na ONU

WSIS – World Summit on the Information Society

Genebra, dez. de 2003 / Túnis, dez. de 2005 www.itu.int/wsis/

WGIG - Working Group on Internet Governance

Genebra, novembro de 2003 a julho 2005 www.wgig.org

IGF – Internet Governance Forum

1º IGF Atenas, Grécia – novembro 2006
2º IGF Rio de Janeiro, Brasil – novembro 2007
3º IGF Hyderabad, India – dezembro 2008
4º IGF Sharm El-Sheik, Egito – novembro 2009
5º IGF Vilna, Lituânia – setembro 2010
6º IGF Nairobi, Quênia – setembro 2011
7º IGF Baku, Azerbaijão – novembro 2012
8º IGF Bali, Indonésia – novembro 2013
9º IGF Istambul, Turquia – setembro 2014
10º IGF João Pessoa, Brasil – novembro 2015
11º IGF Guadalajara, México – novembro 2016
12º IGF Genebra, Suiça – dezembro de 2017
13º IGF Paris, França – novembro de 2018

https://www.intgovforum.org/multilingual/

OTAN

2007 – publicado o *Tallin Manual*

- Análise da legislação aplicável à Guerra Cibernética

2010 – Primeira *International Conference on Cyber Conflict*

- Tópicos discutidos
  - retaliação cinética a ataques cibernéticos
  - legalização do contra-ataque pelo setor privado a redes "proxy" de ataques
    ("proxy" é um eufemismo para qualquer rede origem de um ataque, mesmo uma vítima)
  - estoque de vulnerabilidades

➢ Para pensar: foram "*defense contractors*" de países da OTAN que começaram a usar termos como "*Cyber Defense*", "*Cyber Kill Chain*" e "*Active Defense*" para renomear atividades ou até mesmo tentar tornar "normal" na consciência coletiva que atacar no dia-a-dia é uma forma de proteger...

https://ccdcoe.org/index.html

https://www.youtube.com/user/natoccdcoe/playlists

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

GCCS – *Global Conference on Cyber Space* (aka "*London Process*")

Primeira Conferência em Londres em 2011

- Restrita a Governos
- Criada pelas áreas de política externa e diplomacia
- Objetivo de definir normas de conduta aceitável por Estados no "ciberespaço"

Na Conferência 2015, na Holanda, setor privado foi convidado a participar

- Também foi criado o GFCE – *Global Forum of Cyber Expertise*
  - Grupo formado por Governos, Setor Privado e Organizações Intergovernamentais para focar em "*Capacity Building*"

https://www.thegfce.com/about/gccs

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

- Grupo de 42 países criado após o final da Guerra Fria para controlar a exportação de armas e tecnologias de uso dual

  Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, India, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, Ukraine, United Kingdom and United States.

- 2013 – inserção de "*intrusion software*" na lista de itens controlados
  - ***Scope of the New Entries***

    Systems, equipment, components and software specially designed for the ***generation, operation or delivery of, or communication with, intrusion software*** *include* ***network penetration testing products*** *that use intrusion software to identify vulnerabilities of computers and network-capable devices. Certain penetration testing products are currently classified as encryption items due to their cryptographic and/or cryptanalytic functionality. Technology for the development of intrusion software* ***includes proprietary research on the vulnerabilities and exploitation of computers and network-capable devices****.*

"Cenas dos próximos capítulos" daqui a alguns *slides...*

https://www.federalregister.gov/documents/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items

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 Group of Governmental Experts

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

GCSC - *Global Commission on the Stability of Cyberspace*

- Criada em Janeiro de 2017
- Mantida pelos governos da Holanda, França, Estônia e Cingapura, e por ISOC, PCH, GLOBSEC, Microsoft e Black Hat USA
- Primeiro documento: "*Call to Protect the Public Core of the Internet*"
  https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf
- Missão:

  "[...] ***Conflict between states*** *will take new forms* [...] *increasing* ***the risk of undermining the peaceful use of cyberspace*** *to facilitate the economic growth and the expansion of individual freedoms.*

  In order to counter these developments*, the Global Commission on the Stability of Cyberspace* ***will develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace****.* [...]
- *Plenary Panel: Cyberstability and the Future of the Internet* – NATO CCDCOE CyCon 2017

  Temos que parar de estimular a cultura de "*Cyber Warriors*". Temos que para de falar de ataques e falar de proteção. Segurança real não é "*sexy*" Se eu for atacado com um DDoS eu não vou chamar o "*Cyber Command*" eu vou ligar para o meu ISP. – Jeff Moss

  https://youtu.be/FDBTtawj6Ms

https://cyberstability.org

O que pode dar errado?

"*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* explorando o *EternalBlue*.

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 Recorrentes em Fóruns Globais e Nacionais

cert.br nic.br cgi.br

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*"

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

- acesso excepcional a conteúdo criptografado
- 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**

Acesso Excepcional a Conteúdo Cifrado

Leitura 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.***"

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*" – **aberto a contribuições**
  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/

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

- Cadernos CGI.br - Fórum de Governança da Internet: Relatórios dos dez primeiros anos do IGF
  https://www.cgi.br/publicacao/cadernos-cgibr-forum-de-governanca-da-internet/

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

Obrigada

www.cert.br

cristine@cert.br @certbr

14 de setembro de 2018

nic.br cgi.br

www.nic.br | www.cgi.br