

nic.br cgi.br

cert.br

**10º Seminário de Proteção à
Privacidade e aos Dados Pessoais**
São Paulo, SP
19 de setembro de 2019

Tratamento de Incidentes

- ▶ Articulação
- ▶ Análise Técnica
- ▶ Apoio à recuperação

Treinamento e Conscientização

- ▶ Cursos
- ▶ Palestras
- ▶ Boas Práticas
- ▶ Reuniões

Análise de Tendências

- ▶ *Honeypots* Distribuídos
- ▶ SpamPots
- ▶ Processamento de *threat feeds*



SEI
Partner
Network



Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Foco das Atividades

- Atuar como ponto de contato nacional para notificação de incidentes
- Auxiliar na análise técnica e compreensão de ataques e ameaças
- Estabelecer um trabalho colaborativo com outras entidades
- Aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências
- Transferir o conhecimento adquirido através de cursos, boas práticas e materiais de conscientização

Criação:

Agosto/1996: o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil” é publicado pelo CGI.br¹

Junho/1997: o CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório²

¹<https://www.nic.br/grupo/historico-gts.htm>

²<https://www.nic.br/pagina/gts/157>

O Papel da Criptografia para Garantir a Segurança e a Privacidade

Dra. Cristine Hoepers

Gerente Geral

cristine@cert.br

cert.br **nic.br** **egi.br**

Como conciliar um sistema de normas territoriais às realidades de um cenário digital e interconectado?

- A Internet realmente não tem fronteiras
- Ocultar a fonte dos ataques é muito fácil
- “Atribuição” é muito difícil
- 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
- As leis e normas são territoriais
- Governos historicamente não confiam uns nos outros
- Forças Militares e de Segurança Nacional aplicam a lógica da dissuasão (*deterrence*) no cenário digital
 - “estocar armas” (i.e. vulnerabilidades)
 - [tentar] impedir “inimigos” de ter acesso a estas “armas”
 - espionar todos

Discursos em geral não refletem a verdade dos fatos: **Segurança e privacidade são ambas comprometidas**

“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”

Algumas agências e governos exploram a confusão: 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*
- armazenar *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: Importância da Criptografia

Criptografia

- ciência e a arte de escrever mensagens em forma cifrada ou em código
- é um dos principais mecanismos de segurança

É a base para o funcionamento de:

- certificados e assinaturas digitais
- mecanismos de autenticação
- conexão segura na Web (HTTPS)
- conexão segura para outras aplicações na Internet (SSL/TLS, IPSec)
- proteção de dados armazenados em disco, em mídias removíveis e dispositivos móveis
- integridade de consultas DNS (DNSSEC)

Acesso Excepcional a Conteúdo Cifrado: Possíveis Implementações

Uso de algoritmos “enfraquecidos” que permitam alguns atores a quebrar a criptografia

Uso de chaves mestras (*key escrow*)

- sob guarda das empresas que implementam os produtos ou serviços
- sob guarda de terceiros (polícias, órgãos de governo, agências, etc)

“... the real security challenge is not the mathematics of cryptosystems; it is engineering, specifically the design and implementation of complex software systems.”

– Abelson et. al
Keys Under Doormats

Riscos:

No uso de chaves mestras (1/2)

Vazamento da chave

- não intencional
 - sistemas comprometidos ficarem expostos, falhas nas configurações de sistemas, perda de mídia, erro humano, etc
- intencional

Quem tem a guarda da chave vira alvo e ponto único de falha

- atacantes passam a ter maior incentivo para
 - comprometer a organização
 - recrutar funcionários

Riscos:

No uso de chaves mestras (2/2)

Retroceder a segurança dos sistemas

- inviabiliza o uso da técnica de *Forward Secrecy*
 - hoje é uma técnica amplamente utilizada para garantir que um invasor ou espião não tenha acesso a comunicações anteriores, em caso de comprometimento da chave privada
 - sem *forward secrecy*, se qualquer das chaves privadas for comprometida, imediatamente todos os dados já trocados estão comprometidos

Desafios procedimentais

- Quem terá acesso às chaves mestras?
- Quantas chaves mestras existirão em um país?
- Quais países terão acesso às chaves?
- Como saber se um país não está abusando do acesso para espionar cidadãos de outro país?

Risco adicional:

Criminosos pararem de usar sistemas legítimos

Hoje utilizam os sistemas de mercado

- incentivo para os criminosos: facilidade de uso e de adoção
- vantagem para as autoridades: rapidamente se chega nos meta-dados

Facilmente podem desenvolver seus próprios sistemas

- contratando bons programadores
- usando algoritmos fortes e públicos de criptografia
- mercado “*underground*” online já oferece serviços de programação

- *Russian Underground 101 – Trend Micro*

<http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf>

- *2016 Underground Hacker Markets – Secureworks*

<https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report>

Considerações Finais:

Possíveis Consequências Não Intencionais

Cria-se uma nova superfície de ataque

Incentiva-se o crime organizado a criar seus próprios aplicativos de comunicação, utilizando criptografia forte

Põe-se todos os usuários em risco

- Não é uma questão de “se” atores maliciosos terão acesso aos sistemas que guardam as chaves ou o texto em claro
- Mas sim de o que fazer “quando” eles tiverem acesso

A sociedade perde a confiança na tecnologia

- Inibe-se a inovação
- Reduz-se a qualidade de vida

Acesso Excepcional a Conteúdo Cifrado:

Referências

- *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.**”*

- *The Second Crypto War—What's Different Now*

Susan Landau, *Bridge Professor of Cyber Security and Policy, Tufts University*

<https://www.usenix.org/conference/usenixsecurity18/presentation/landau>

(Slides, Áudio e Vídeo disponíveis no *link* acima)

Referências Adicionais

The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)

<https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=30310>

Cartilha de Segurança para a Internet

<https://cartilha.cert.br/>

Security Engineering, 2nd Edition, 2008, Ross Anderson

<http://www.cl.cam.ac.uk/~rja14/book.html>

Cyber Risk and Resilience Management, CERT/CC

<http://www.cert.org/resilience/>

Obrigada

✉ cristine@cert.br

✉ Notificações para: cert@cert.br

📧 @certbr

www.cert.br

19 de setembro de 2019

nic.br **cgi.br**

www.nic.br | www.cgi.br