nic.br cgi.br | cert.br

**Seminário de Proteção à Privacidade e aos Dados Pessoais**

**São Paulo, SP**

24 de agosto de 2016

# Criptografia: Privacidade e Segurança ou Privacidade vs. Segurança?

**Cristine Hoepers, D.Sc.**
**Gerente Geral**

cert.br nic.br cgi.br

# O que vem à mente quando pensamos em invasão de privacidade?

# A privacidade e a segurança estão cada vez mais nas mãos de terceiros

**Privacidade com relação ao que está no dispositivo do usuário e ao que ele faz na Internet – em tese ele teria controle sobre esses dados**

- dados armazenados
- acessos a *sites* e conteúdos
  - gostos, hábitos, opiniões

**Privacidade com relação a dados que precisam estar nos computadores de terceiros ou trafegar pela rede**

- depende destes terceiros manterem a confidencialidade
- serviços de *e-gov*, *e-health*, *e-commerce, e-**
  - resultados *online* de exames, serviços de previdência, cartões de crédito, *sites* de nota fiscal, dados biométricos, RFIDs em carros e passaportes, preferências e histórico de compras, etc

**Estes dados estão protegidos?**

➢ exemplos crescentes de problemas...

International Business Times

from US-based email accounts including Gmail, Yahoo or Hotmail for just $129 (£92). Hacking into someone's corporate email account will cost $500

# Hackers can break into your Gmail, Hotmail or Yahoo account for just $129, says Dell

*By Hyacinth Mascarenhas*

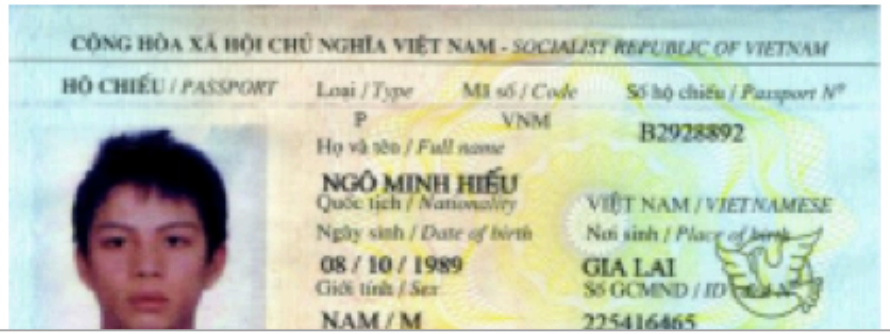
*April 8, 2016 06:40 BST*

Prices for a Remote Access Trojan (RAT) — a malware program that allows cybercriminals to secretly control your computer remotely — are dirt cheap, going for as little as $5 to $10. An Angler Exploit Kit, on the other hand, costs between $100 and $135. DDoS attacks are usually charged by the hour, day or week and range from $5 to $555. Doxing goes for $20. Hacking tutorials are also available for purchase online for criminals on a budget and goes for as little as $20-$40.

http://www.ibtimes.co.uk/hackers-can-break-into-your-gmail-hotmail-yahoo-account-just-129-says-dell-1553764#cid=885696

# 10 MAR 14 Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records

In October 2013, KrebsOnSecurity published an exclusive story detailing how a Vietnamese man running an online identity theft service bought personal and financial records on Americans directly from a company owned by **Experian**, one of the three major U.S. credit bureaus. Today's story looks deeper at the damage wrought in this colossal misstep by one of the nation's largest data brokers.




Last week, **Hieu Minh Ngo**, a 24-year-old Vietnamese national, pleaded guilty to running an identity theft service out of his home in Vietnam. Ngo was arrested last year in Guam by **U.S. Secret Service**

Experian came into the picture in March 2012, when it purchased Court Ventures (along with all of its customers — including Mr. Ngo). For almost ten months after Experian completed that acquisition, Ngo continued siphoning consumer data and making his wire transfers.

BBC | Sign in | News | Sport | Weather | Shop | Earth | Travel | M

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts

Technology

# Osram Lightify light bulbs 'vulnerable to hack'

27 July 2016 | T

**Security researchers have discovered nine vulnerabilities in a range of internet-connected light bulbs made by Osram.**

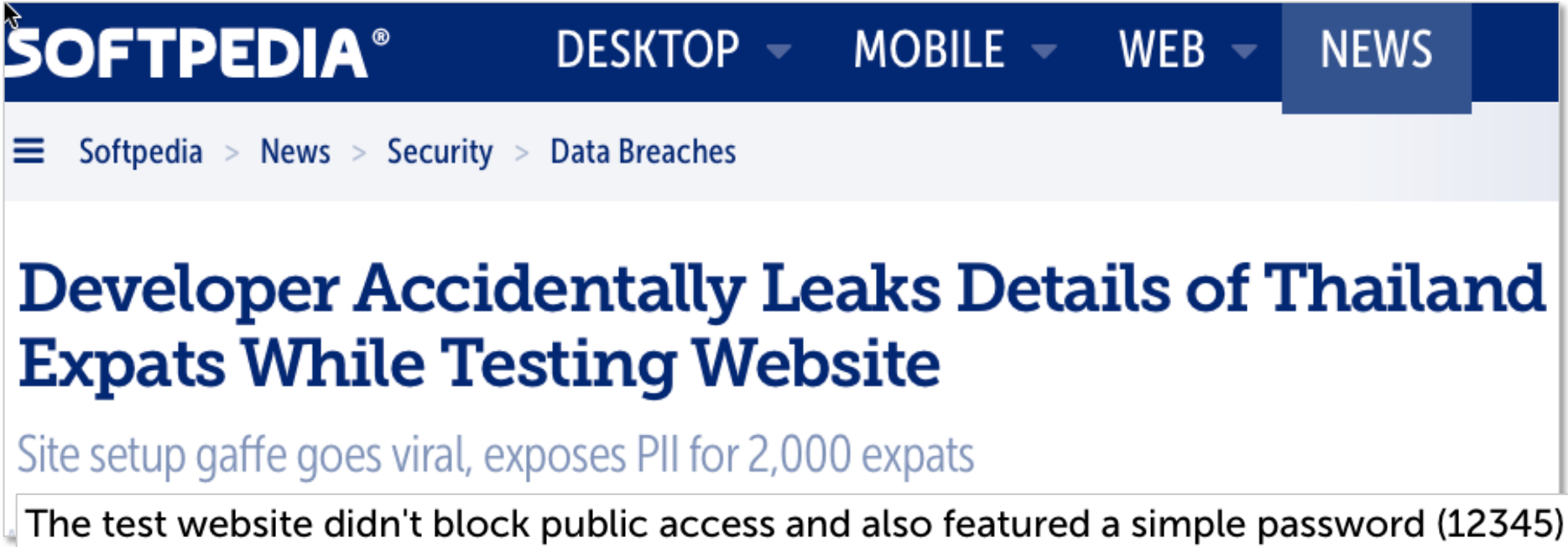
The flaws in the Lightify products could give attackers access to a home wi-fi network, and potentially operate the lights without permission.

Osram said a "majority" of the problems would be fixed in a software update in August, but four remained unpatched.

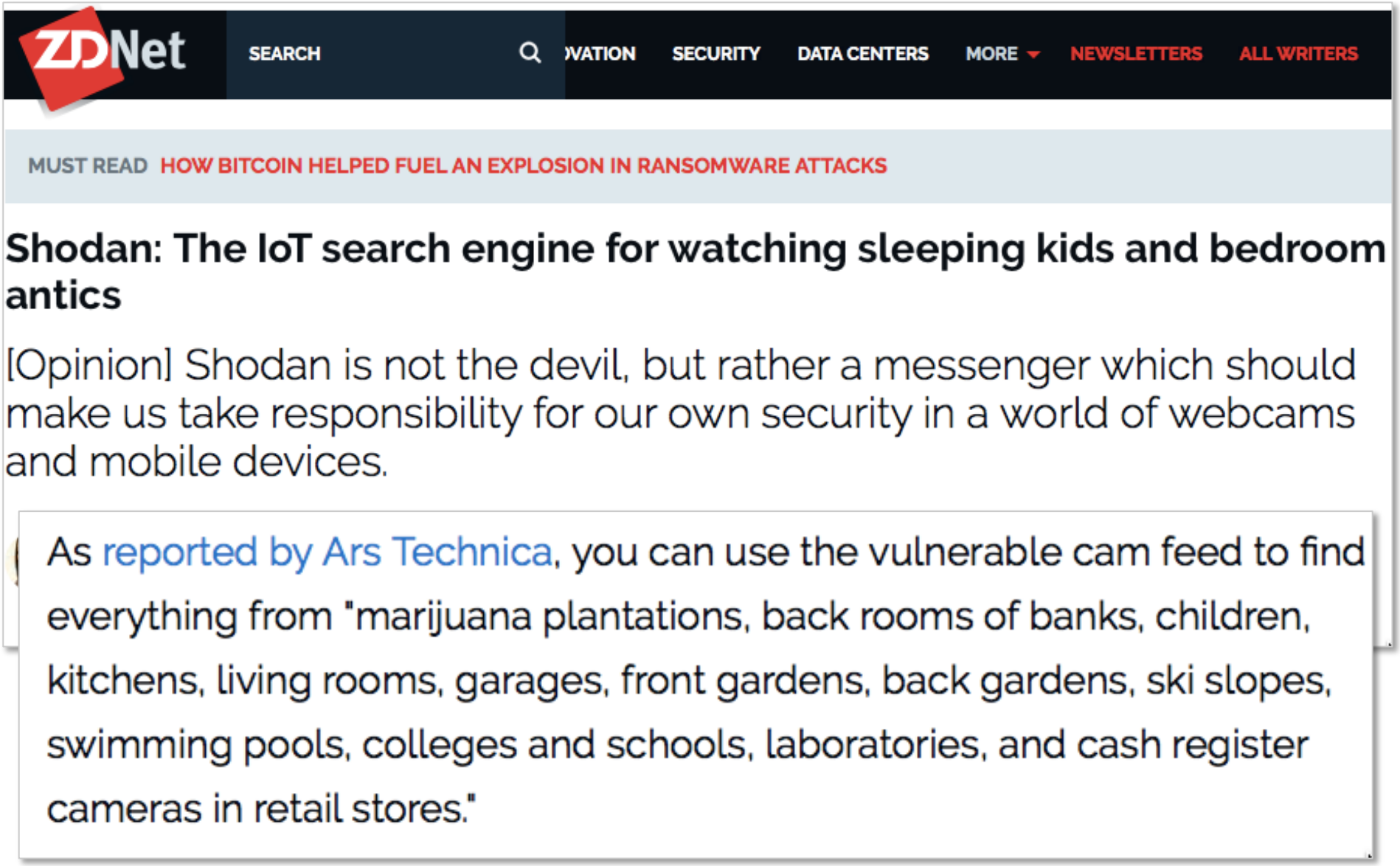
One security expert said Osram had made an "elementary" mistake.

http://www.bbc.com/news/technology-36903274


https://labs.bitdefender.com/2016/08/hackers-can-use-smart-sockets-to-shut-down-critical-systems/




http://news.softpedia.com/news/developer-accidentally-leaks-details-of-thailand-expats-while-testing-website-502287.shtml




http://www.zdnet.com/article/shodan-the-iot-search-engine-which-shows-us-sleeping-kids-and-how-we-throw-away-our-privacy/

# Thousands of medical devices are vulnerable to hacking, security researchers

The security flaws put patients' health

James Niccolai Sep 29, 2015 5:50 PM
IDG News Service

Next time you go for an MRI scan, remember that the doctor might not be the only one who sees your results.

Thousands
infusion pur
security res

The same default passwords were used over and over for different models of a device, and in some cases a manufacturer warned customers that if they changed default passwords they might not be eligible for support. That's


http://www.pcworld.com/article/2987813/thousands-of-medical-devices-are-vulnerable-to-hacking-security-researchers-say.html

# Privacidade é prejudicada com o cenário atual

**Crescente demanda por serviços *online***

- Sistemas estão cada vez mais interconectados e interdependentes
- Dados sensíveis estão mais expostos
  - por necessidade, comodidade ou descuido

**Segurança não é prioridade**

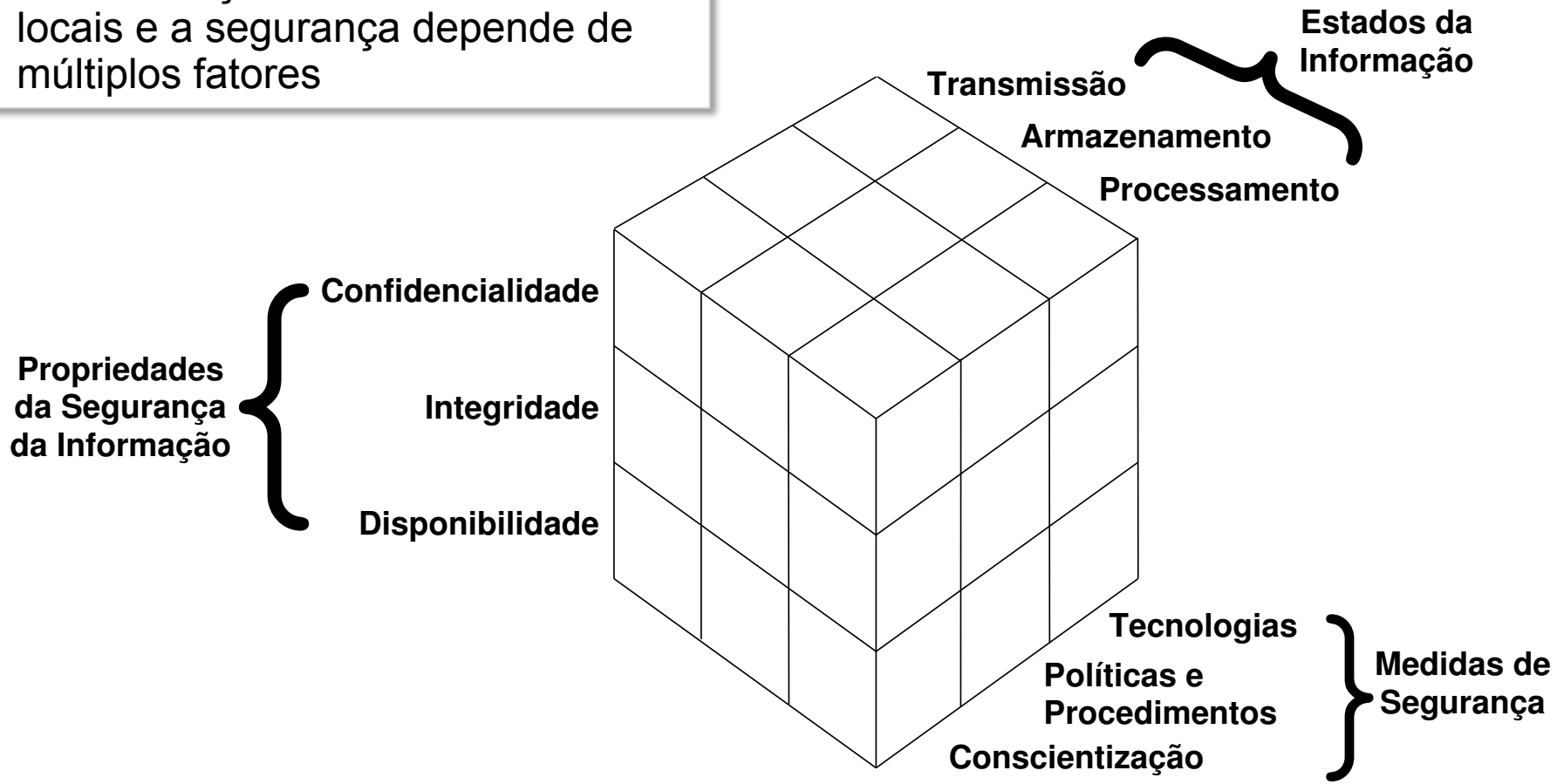
- Impactos não são compreendidos
- Inocência dos desenvolvedores sobre impacto das decisões
- Segurança não é parte do projeto e desenvolvimento
  - "alguém outro vai implementar"
- Dados tem muito valor para o crime organizado
  - bases de dados ("*big data*")
  - sistemas de e-gov
  - infraestruturas críticas
  - dados médicos

# Mas, tecnicamente, como proteger a privacidade?

cert.br nic.br cgi.br

# Segurança da Informação

- De maneira simplificada, tudo que queremos proteger são informações
- 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/

# Em Segurança da Informação: **Privacidade e 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.


**Security Engineering — The Book, Ross Anderson, Cambridge University**
**ISBN:** 978-0470068526 **–** http://www.cl.cam.ac.uk/~rja14/book.html

# Importância da Criptografia

**Criptografia**

- ciência e arte de escrever mensagens em forma cifrada ou em código
- é uma das principais tecnologias 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)

**Cartilha de Segurança para a Internet, Capítulo 9**
**ISBN:** 978-85-60062-54-6 **–** http://cartilha.cert.br/livro/

# O que se ouve na suposta batalha: **Segurança vs. Privacidade**

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

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

"*Usar criptografia em tudo garante privacidade*"

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

"*Para ter privacidade deve-se eliminar*

- *logs*
- *cookies*"

# Não confundir:
# **Segurança com Controle**

## Medidas de Controle

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

## Medidas de Segurança

- 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
- criptografia sem “chaves mestras”


Os ministros do Interior de França, Bernard Cazeneuve, e Alemanha, Thomas De Maizière, anunciaram na terça-feira, 23, que solicitarão à Comissão Europeia que crie uma legislação para obrigar as operadoras de telecomunicações e empresas de software a quebrarem o sigilo de conteúdos criptografados em caso de investigações judiciais que envolvam, por exemplo, suspeitas de atividade terrorista, se quiserem continuar atuando no mercado europeu.

http://internacional.estadao.com.br/noticias/geral,europa-debate-sigilo-de-whatsapp-e-telegram,10000071569

ZDNet MENU US

# Microsoft Secure Boot key debacle causes security panic

Security failures have created "golden keys" which unlock Windows devices protected by Secure Boot. [Updated]

By Charlie Osborne for Zero Day | August 10, 2016 -- 10:26 GMT (03:26 PDT) | Topic: Security

"About the FBI: are you reading this? If you are, then this is a perfect real world example about why your idea of backdooring cryptosystems with a "secure golden key" is very bad!," the team added. "Microsoft implemented a "secure golden key" system. And the golden keys got released from MS['s] own stupidity."

http://www.zdnet.com/article/microsoft-secure-boot-key-debacle-causes-security-panic/

# Leitura obrigatória sobre este tema

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

**Author:** Abelson, Harold; Anderson, Ross; Bellovin, Steven M.; Benaloh, Josh; Blaze, Matt; Diffie, Whitfield; Gilmore, John; Green, Matthew; Landau, Susan; Neumann, Peter G.; Rivest, Ronald L.; Schiller, Jeffrey I.; Schneier, Bruce; Specter, Michael; Weitzner, Daniel J.

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.*"

# Obrigada

www.cert.br

cristine@cert.br

@certbr

24 de agosto de 2016

nic.br cgi.br

www.nic.br | www.cgi.br