ACME! Cybersecurity Research

GTER 40
GTS 26

# Desenvolvimento vs Segurança?

Vinícius Oliveira Ferreira

viniciusoliveira@acmesecurity.org

SecurityIN
Security into your software

# Sobre o autor

- Vinícius Oliveira Ferreira:
  - Pesquisador e analista no Laboratório ACME!
  - Mestrando em Ciência da Computação pela UNESP – Universidade Estadual Paulista.
  - Bolsista CAPES.
  - Idealizador da iniciativa *securityin.com.br*

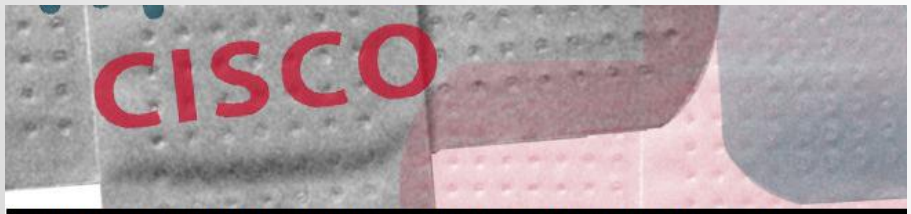
SecurityIN
Security into your software

ACME!
Cybersecurity Research

unesp

# Um problema não resolvido

APPLE PATCHES 50 VULNERABILITIES ACROSS IOS, OS X, SAFARI




CISCO WARNING OF VULNERABILITIES IN ROUTERS, DATA CENTER PLATFORMS

NEWS

## Adobe updates Flash Player to patch 23 flaws

## HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

## Known Security Flaw Found In More Antivirus Products

A vulnerability discovered earlier this year in AVG software also spotted in Intel McAfee, Kaspersky Lab AV products.

## Zero-Day Vulnerabilities Found In Kaspersky, FireEye Anti-Virus Software: Two Researchers Reveal Major Flaws In Security Products

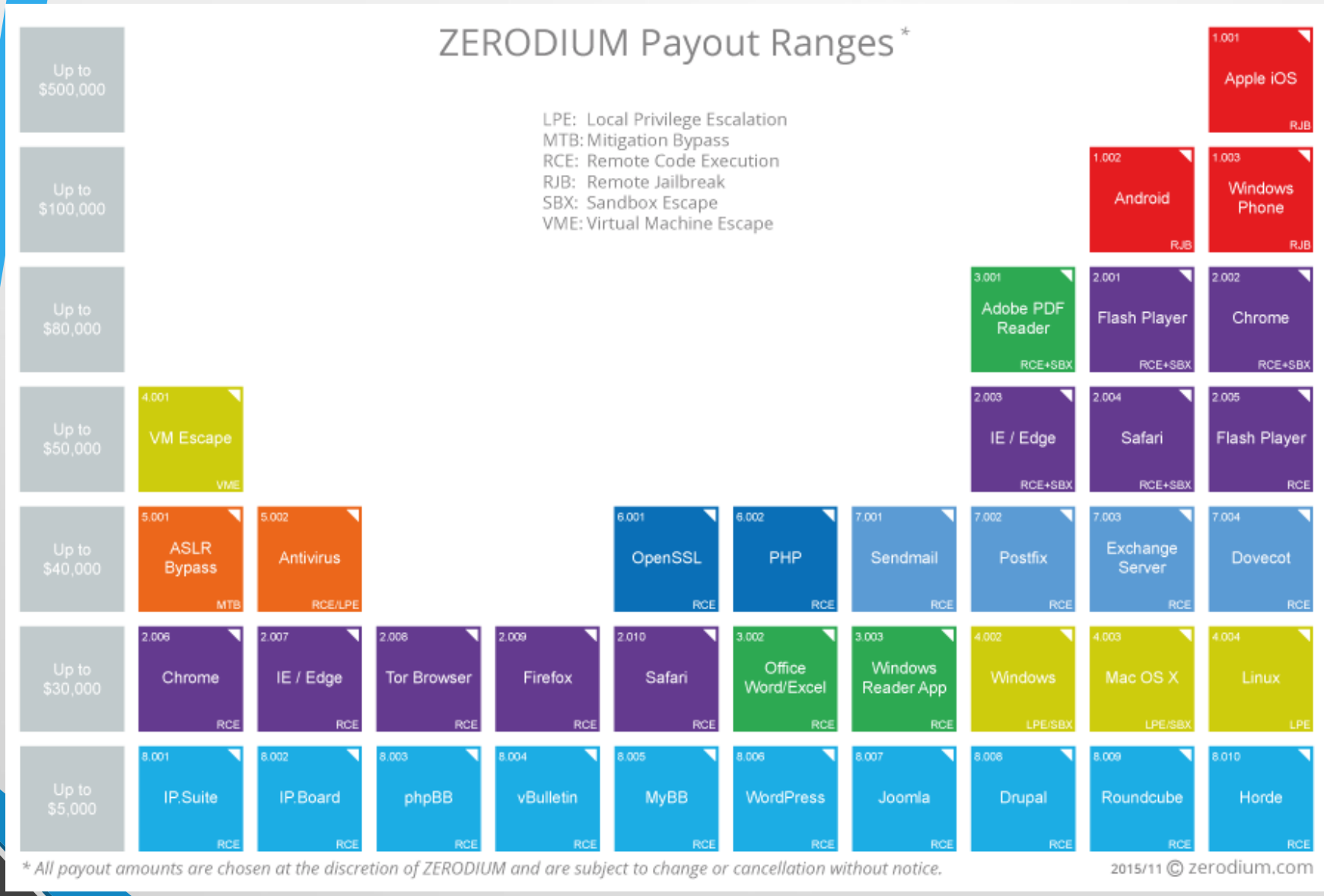
# Um problema não resolvido

- MITRE adota nova sintaxe ao padrão *Common Vulnerabilities and Exposures* (CVE):

| **IDs with 4 digits** | **IDs with 5 digits** (when needed) | **IDs with 6 digits** (when needed) | **IDs with 7 digits** (when needed) |
|---|---|---|---|
| CVE-2014-0001 | CVE-2014-10000 | CVE-2014-100000 | CVE-2014-1000000 |
| CVE-2014-3127 | CVE-2014-54321 | CVE-2014-456132 | CVE-2014-7654321 |
| CVE-2014-9999 | CVE-2014-99999 | CVE-2014-999999 | CVE-2014-9999999 |

**NOTE:** Some of the CVE-ID examples above have not yet been assigned.

**Nova sintaxe para o padrão CVE. Figura extraída de [1].**



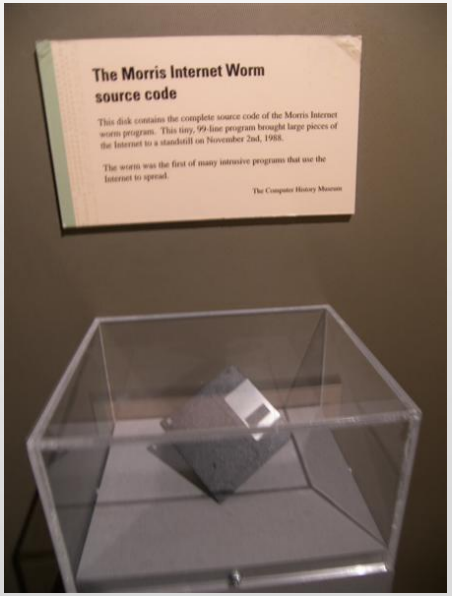

**Lista de valores pagos a *exploits* o-day. Figura extraída de zerodium.com/program.html**

# *Priests vs Acolytes*

- Historicamente a segurança tem sido regida pelos administradores de rede e servidores. Os desenvolvedores ainda não desempenharam um protagonismo considerável na área.

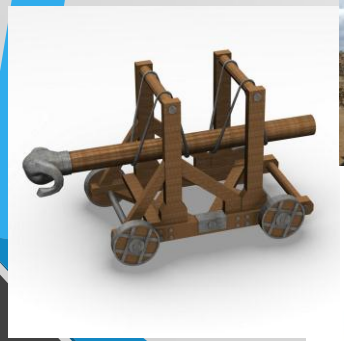
# Segurança de perímetro

- Como consequência a segurança foi desenvolvida de acordo com suas visões e expertise.
  - Desenvolvimento da segurança de perímetro com o estabelecimento do *Firewall*, seu desenvolvimento foi catalisado pela disseminação do *worm* de Morris em 1988.



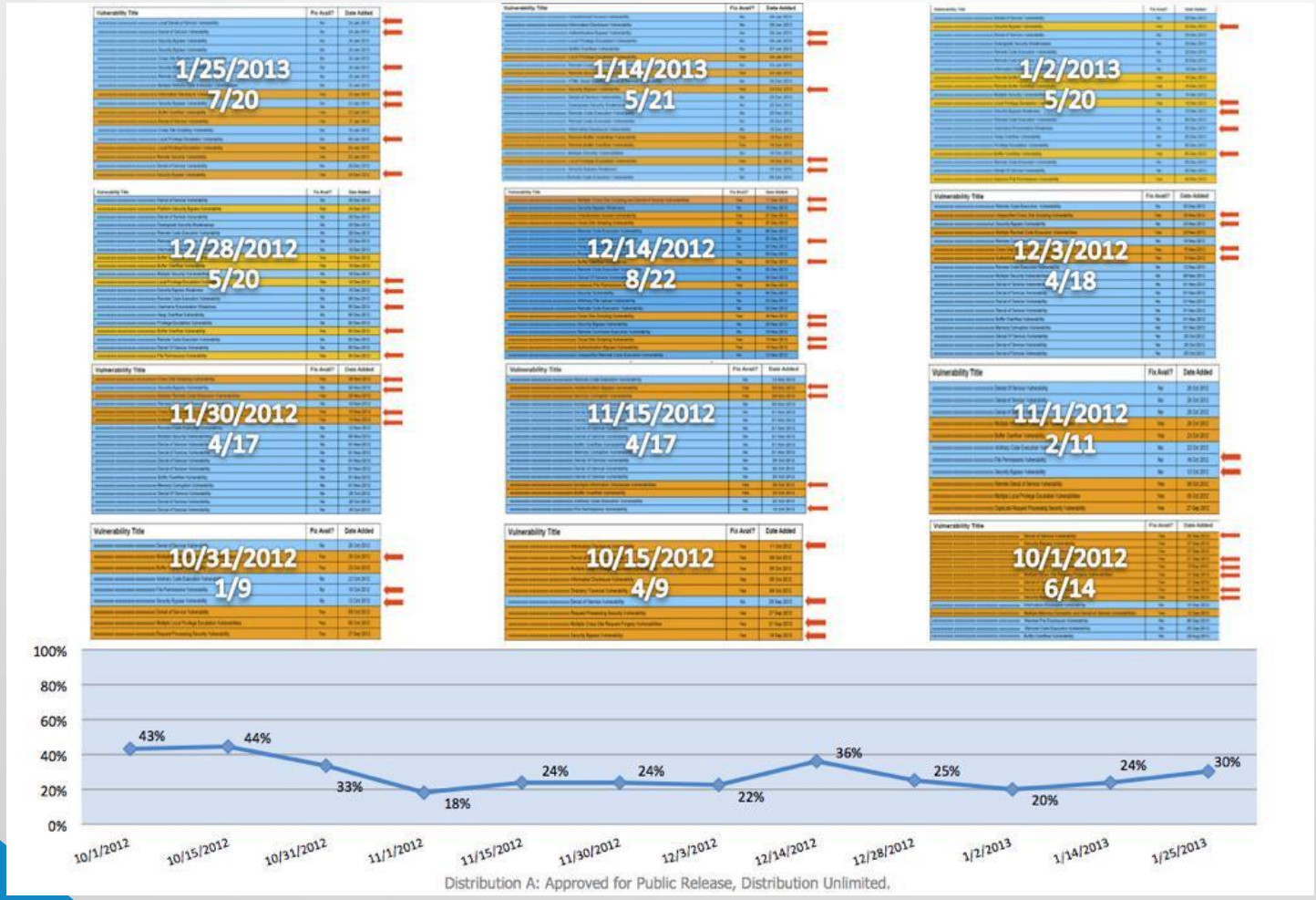
# Segurança de perímetro

# Como a segurança de perímetro tem falhado?



# O que é o perímetro hoje?

# As ferramentas que protegem o perímetro são SW!

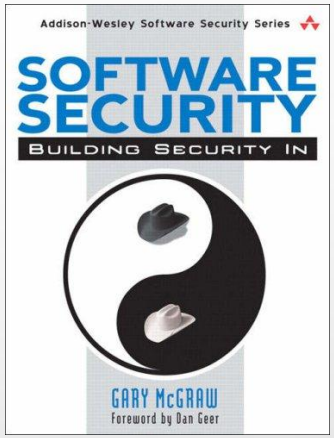


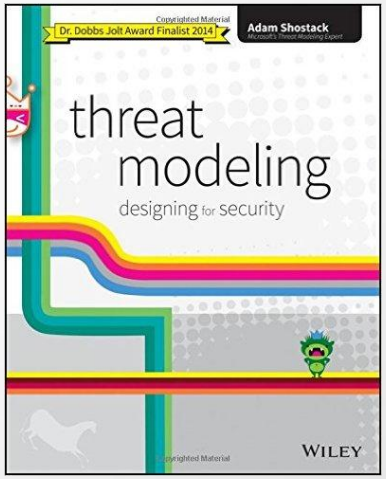

**1/3 das vulnerabilidades nos sistemas do governo americano foram encontradas em sistemas de segurança. Via @dotMudge.**

# A dissolução do perímetro

- A segurança de perímetro não foi suficiente.
  - É preciso tratar o elo mais fraco desta cadeia, o **SOFTWARE.**

# Algumas iniciativas

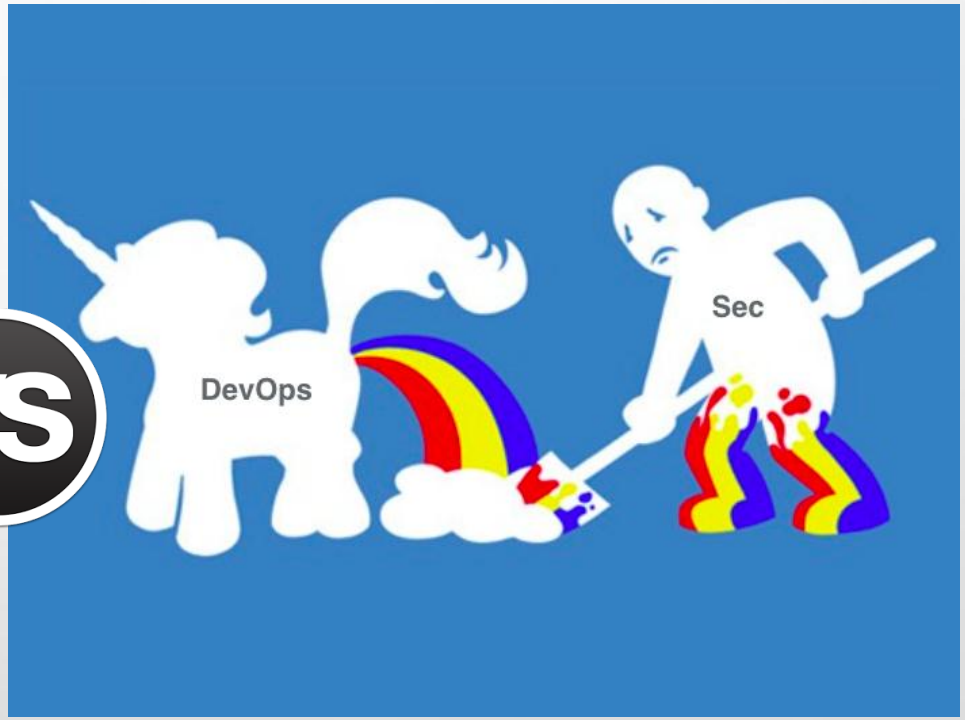


**ISO/IEC 27034**


# Mas, quem é que vai fazer isso?

# Mas, quem é que vai fazer isso?

VS



# Quem é o responsável?

SecurityIN
Security into your software

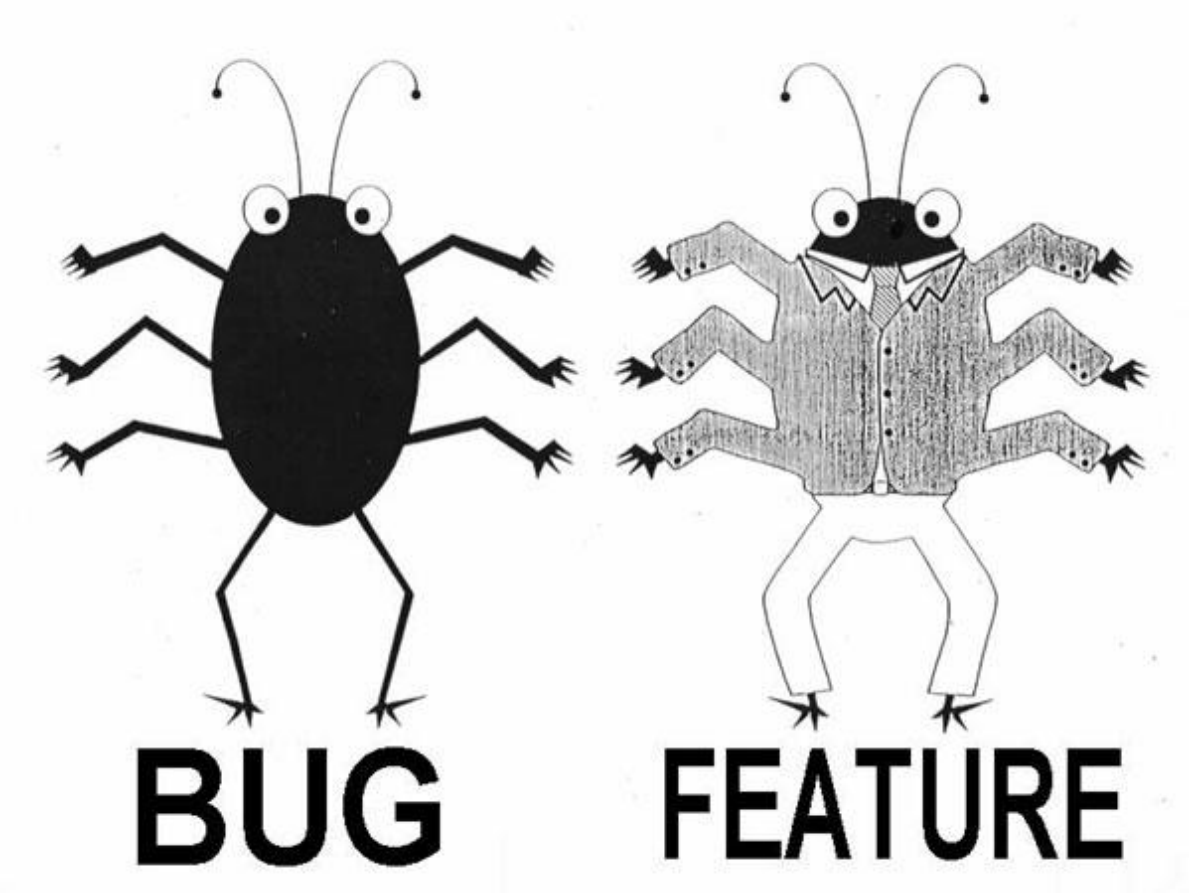
# Nós não somos os agentes de mudança!

# *The Principal-Agent Problem*

- Incentivos conflitantes entre um principal que contrata um agente para desempenhar uma tarefa específica;
- A falta de alinhamento de incentivos é um grande problema em vários ramos da economia;
- Há um claro conflito de incentivos ao tratarmos de segurança e desenvolvimento no contexto atual.

# *The Principal-Agent Problem*

# *The Principal-Agent Problem*



# *The Principal-Agent Problem*

- Como resolver:
  - Alinhando os incentivos dos principais e agentes de modo a se criar complementaridade e não oposição.
  - Algumas soluções encontradas:
    - Elaboração de contratos mais detalhados;
    - Rever as formas de recompensar os agentes;
    - Exigência de garantias;
    - Meios eficientes de 'monitorar' o desempenho dos agentes.

# Alinhando os Incentivos

SecurityIN
Security into your software

# Segurança *TOP-DOWN*

O desenvolvimento sempre dança conforme a música

# Compreendendo os riscos

- *Ex:* Microsoft
  - Atingida pelo Code RED em 2001.
    - O *worm* explorava uma vulnerabilidade no Microsoft ISS Web Server.
    - O pico de infecções ocorreu em 19-07 com mais de 350 mil infecções em menos de 14 horas.

SecurityIN
Security into your software

# Compreendendo os riscos


**Queda no valor das ações da *Microsoft* após o *Code Red*. Gráfico gerado por Yahoo Finance.**

# Compreendendo os riscos

- *Ex:* Microsoft
  - Motivada, em grande parte pelo incidente com o Code Red, Bill Gates lança no início de 2002 seu famoso memorando: *Trustworthy Computing.*

*So now, when we face a choice between* ***adding features*** *and resolving* ***security issues****, we need to choose* ***security****.* – **Bill Gates, The Trustworthy Computing Memo.**

# Compreendendo os riscos



Microsoft®
Security Development Lifecycle
Process Template

# Uma exigência de mercado

- Novos recursos/funcionalidades são mais apelativos, em contrapartida a segurança é quase sempre invisível.
  - No entanto, os consumidores sempre esperam estar adquirindo um produto seguro. É instintivo que a segurança seja considerada uma premissa básica.

SecurityIN
Security into your software

# Responsabilidade legal

## General Motors pagará multa de US$ 1 bilhão por defeito

20

EFE: 16/09/2015 | 21h13

The Washington Post

## U.S. Fines Firestone $500,000

THE WALL STREET JOURNAL.

Subscribe Now | Sign In

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate Search


Anglo American to Slash Assets, Cut 85,000 Jobs

Antitrust Cops Put Brakes on Staples, GE Deals


Architect of Valeant's Turnaround Is Under Fire


'Star Wars' Carries Its Own Marketing Weight for Disney


New Rubber in Merge

109

BUSINESS

## U.S. Fines Honda $70 Million for Failing to Report Safety Issues

Penalties Are Highest Levied Against an Auto Maker by Auto-Safety Regulator

# Responsabilidade legal


REUTERS EDITION: U.S. SIGN IN | REGISTER Search Reuters

HOME BUSINESS MARKETS WORLD POLITICS TECH OPINION BREAKINGVIEWS MONEY LIFE PICTURES VIDEO

ADVERTISEMENT

**Landing** | Mon Aug 24, 2015 1:32pm EDT Related: WORLD, TECH, CYBER

## Two people may have committed suicide after Ashley Madison hack: police

TORONTO | BY ALASTAIR SHARP

# Adoção de Seguro Cibernético

*Today, network security insurance is a rarity-very few of our customers have such policies-but eventually it will be commonplace* – **Bruce Schneier, 2004**.

# Adoção de Seguro Cibernético

Crescimento dos valores investidos em prêmios de Seguro Cibernético


Gráfico construído com informações obtidas em [2] e [3].

# Adoção de Seguro Cibernético

- O nicho que mais cresce dentro da indústria de seguros [4].
- As vendas da Marsh têm crescido acima de 30% nos dois últimos anos [5] [6].
- Todas as grandes seguradoras já oferecem este serviço: American International Group, Chubb, Ace, Allianz.
- 6 entre 10 gestores de TI contrataram este serviço em 2015 [7].

# Adoção de Seguro Cibernético

- A indústria de seguro cibernético deve reger a indústria de segurança nos próximos anos.
  - Por meio de uma redução de taxas, as seguradoras incentivarão os gestores a adotarem determinados produtos/serviços de segurança.
  - Uma vez que as seguradoras arcarão com as perdas, a escolha desses produtos deverá ser racional.
  - Isso tende a eliminar o *Market for Lemons* existente na indústria de segurança, incentivando-as na **criação de produtos robustos**.

SecurityIN
Security into your software

# Adoção de Seguro Cibernético

*Insurance companies will look to security processes* ***that they can rely on: process of secure software development before systems are released****, and the processes of protection, detections…* – ***Bruce Schneier, 2004.***

# Conclusões

## The Rugged Manifesto

# The Rugged Manifesto

Eu sou robusto e, mais importante, o meu código é robusto.

Eu reconheço que o software se tornou uma fundação de nosso mundo moderno.

Eu reconheço a enorme responsabilidade que vem com este papel fundamental.

Eu reconheço que meu código será usado de maneiras que eu não posso prever, de forma que não foi concebido, e por mais tempo do que jamais foi destinado. Eu reconheço que meu código será atacado por adversários talentosos e persistentes que ameaçam a nossa segurança física, econômica e nacional.

Eu reconheço essas coisas - e eu escolhi ser robusto.

Eu sou robusto porque me recuso a ser uma fonte de vulnerabilidades ou fraqueza. Eu sou robusto porque eu garanto que meu código irá suportar sua missão.

Eu sou robusto porque o meu código pode enfrentar esses desafios e persistir apesar deles.

Eu sou robusto, não porque é fácil, mas porque é necessário e estou pronto para o desafio.

# Referências

[1] CVE-ID Syntax Change. Disponível em: <https://cve.mitre.org/cve/identifiers/syntaxchange.html>. Acesso em:  8 de dezembro de 2015.

[2] VISION 2025 AND AAMGA. Disponível em: <https://www.lloyds.com/news-and-insight/press-centre/speeches/2015/05/vision-2025-and-aamga>. Acesso em:  8 de dezembro de 2015.

[3] Cyber insurance market set to reach $7.5 billion by 2020. Disponível em: <http://pwc.blogs.com/press_room/2015/09/cyber-insurance-market-set-to-reach-75-billion-by-2020-pwc-report.html>. Acesso em:  8 de dezembro de 2015.

# Referências

[4] Cyberattack Insurance a Challenge for Business. Disponível em: <http://www.nytimes.com/2014/06/09/business/cyberattack-insurance-a-challenge-for-business.html?_r=0>. Acesso em:  8 de dezembro de 2015.

[5] MARSH. Benchmarking Trends: As Cyber Concerns Broaden, Insurance Purchases Rise.

[6] MARSH. Benchmarking Trends: Cyber-Attacks Drive Insurance Purchases For New and Existing Buyers.

[7] The Global State of Information Security® Survey 2016.

# Thank You!



Vinicius Oliveira Ferreira


@viniciusofer


SECURITYIN
Security into your software