



Pro-active application Security

Sebastien Deleersnyder
CISSP CISA CISM
Manager Application Security

Confidential

September 10, 2008

1



Who Am I?

- 5 years developer experience
- 8 years information security experience
- Lead application security @ Telindus, Belgacom ICT
- Belgian OWASP Chapter Founder / OWASP Board Member

In Commercial Confidence

Security is more than Technology!

A solution is a "package" that could contain:

Consultancy

Integration

Management

..taking into account 3 points of view:

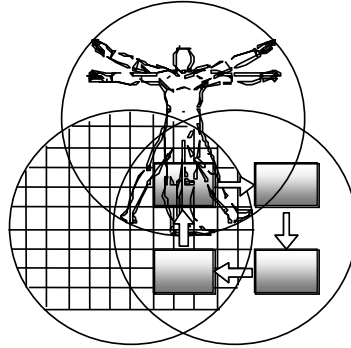
People

Processes

Technology

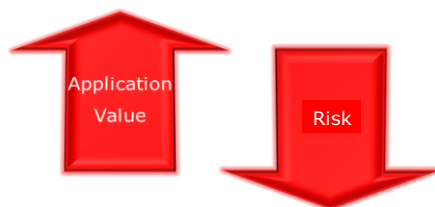
...that will mitigate your business risks

By Solving C.I.A. Issues and Threats



Application Security

Application security is the use of services and technology to protect critical business applications from external threats.



Web application (in)security

Attacks: 75% Application

Applications: 3 out of 4 Vulnerable

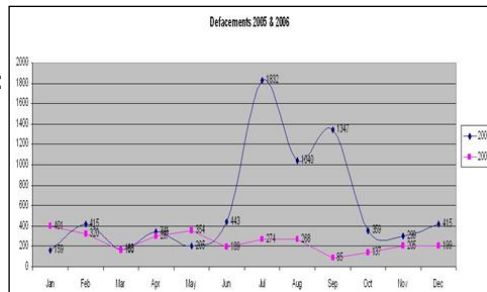
Security defect: 6 hours to fix (average)

Belgium Web Sites defaced:

2005: **2889**

2006: **7023**

* Zone-H



Hacktivism: defacements...

Own3d by Cyber-Terrorist

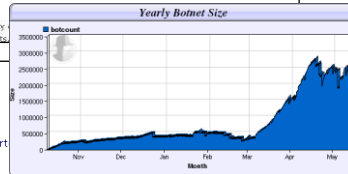


Making money

- Steal Credit Cards
- Bot-Net Pharming
- Sell Phishing Tools
- Identity Theft

Robust International Market for Stolen Credit-Card Numbers
 Ten dollars for a social security number
 By: Kerry Mundak
 Comments: 0
 Think of it as sort-of a smorgasbord. For one dollar, a thief can purchase a stolen credit card number. He could buy it from another thief in one of hundreds of online, international chat-rooms set-up for that purpose. For three dollars, he could buy the credit card number with the three digit security code. For five dollars, he could also receive the number for the card and the name on the card. For ten dollars, he could buy the cardholder's social security number and mother's maiden name.

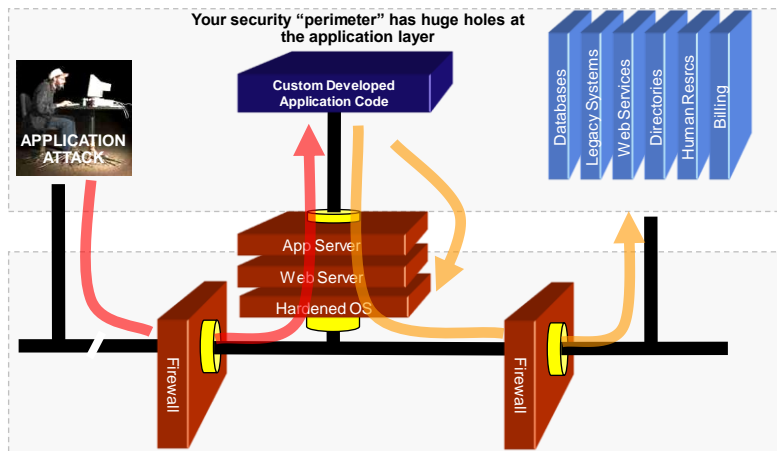
Russian mafia hackers loot ebusinesses
 By Pete Morris (09-03-2001)
 Lax IT managers have been blamed for a series of attacks throughout the world.
Security -> Ian Lynch (15 Aug 2000)
Bloomberg blackmail hacker suspects held
 Two alleged hackers from the former Soviet state of Kazakhstan have been arrested in connection with a report of a blackmail attempt against financial information service provider Bloomberg.
 According to reports in the New York Times, a man calling himself Alex, who said he had obtained passwords of senior Bloomberg employees, contacted chief executive Michael Bloomberg in March.
 The FBI (NIPC) said yesterday that more than 40 US Companies had been targeted in more than 20 states. It said



- 20 nov - Monster.com infections - Neosploit exploit package
- 12 nov - India Times - 434 malwares - Scansafe blocked
- 22 Jan - Legitimate Web sites compromised by attackers made up the majority of sites used to spread malicious programs

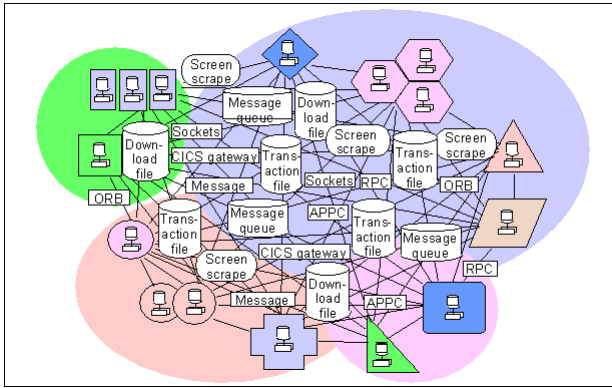
10 September 2008

Problem illustration



Firewall, SSL, IDS, hardening do not stop or detect application layer attacks

Making it harder



complexity



spaghetti code

Confidential

September 10, 2008

9

Making it even more harder



need for bells and whistles



no appsec awareness /training

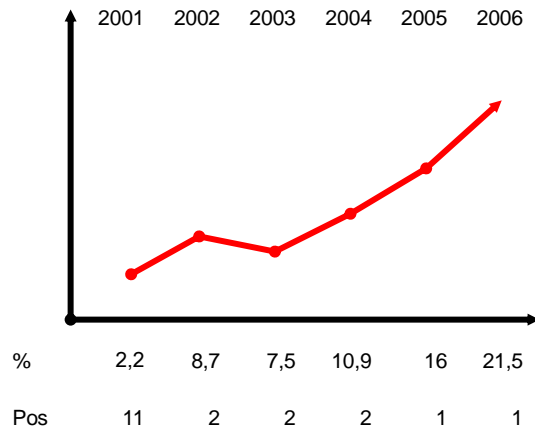


Confidential

Problem size?

#1

CVE



Confidential - Internal Use ONLY

10 September 2008 | slide 11

XSS in 7 major Dutch online banks (royald)

Betalen Sparen Internetbankieren Hypotheken

home > klantenservice > zoekresultaten

Zoekresultaten

Resultaten voor ">alert('XSS');</script>"

The page at http://www.postbank.nl says: XSS

Postbank

rmuleer uw vraag opnieuw

irorekening aan?
gnummer of inlogcod

jn Girorekening?

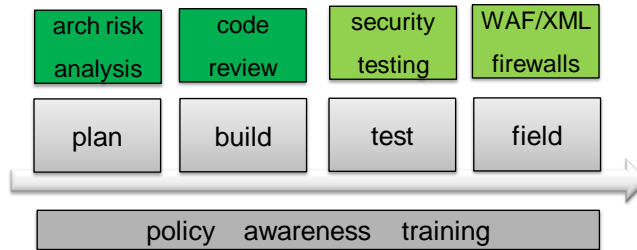
Postbank
ABN AMRO
SNS bank
Fortis banking

Delta Lloyd banking
Sparbeleg banking
Insinger de Beaufort banking

Source: 0x000000.com 12

Pro-active action!

360° approach for secure applications
application security **end-2-end protection**:



People

Awareness decision makers

- Board of Directors
- Audit and Assurance (Risk Management)
- CEO/CFO/CIO
- Executive(s) responsible for systems development and change management
- Sales, Marketing & Product Management!

Developers

- Developer awareness
- Secure design guidelines
- Secure implementation practices

Risk analysis – Threat modeling

Organisation level - risk analysis:

- Perform business impact/risk analysis
- Identify critical business applications
- Focus on business risks
- Ownership?

Application level – threat modeling:

- What are the real threats against the application?
- Focus on technical threats

In Commercial Confidence

Threat modeling

Select mitigation strategy & techniques based on identified, documented and rated threats.

Benefits:

- Prevent security design flaws
- Identify & address greatest risks
- Increased risk awareness and understanding
- Mechanism for reaching consensus
- Cost justification and support for needed controls
- Means for communicating results

In Commercial Confidence

Code review

Secure coding guidelines (e.g. OWASP Guide)
Security bugs subset of implementation bugs!
Static / dynamic analysis tools
Requires manual inspection

Benefits:

- Improves code quality
- Prevents security bugs
- Increased developer awareness and understanding

In Commercial Confidence

Application Security Testing

Focus on application vulnerabilities
Tools can do the automated work
Experienced testers needed
Black / white Box security testing
Multi-level report:

- Technical details
- Analysis
- Management summary

Benefits:

- Foundation for metrics
- Found problems are symptoms, not only fix list!

In Commercial Confidence

Deployment process

Ensure the application configuration is secure

Ensure monitoring of the application security alerts

Security is increasingly “data-driven”

XML files, property files, scripts, databases, directories

How do you control and audit this data?

Design configuration data for audit

Put all configuration data in change management

Audit configuration data regularly

Don't allow configuration changes in the field

Gap development – deployment!

In Commercial Confidence

Web Application / XML firewall

Quick reaction capability

Monitor, block and report attacks & anomalies

Offload crypto / authentication

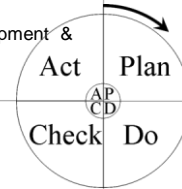
Protection of legacy / 3rd party applications

Benefit:

Buy time in case of vulnerabilities

Application Security Assurance Framework

Quality	Application Security
ISO standards Industry level	Standards / Best Practices: ISO 17799:2005, CoBIT, COSO, NIST, Microsoft SDL, OWASP CLASP and DHS BSI
Quality Assurance Company level	Application Security Assurance Set up AppSec Assurance Framework for Development & Deployment Process
Quality Control Project level	AppSec Controls Part of development <u>and</u> deployment of one application



In Commercial Confidence

Application Security Defect Tracking and Metrics

“Every security flaw is a process problem”

Tracking security defects

Find the source of the problem

Bad or missed requirement, design flaw, poor implementation, etc...

Issue: can you track security defects the same way as other defects?

Metrics

What lifecycle stage are most flaws originating in?

What security mechanisms are we having trouble implementing?

What security vulnerabilities are we having trouble avoiding?

In Commercial Confidence

Change the game!

